

Terms and Conditions
for COOPERATIVE AGREEMENT
Sikes Act Authority
13 December 2021

AUTHORITY

This agreement is being awarded under the authority of the Sikes Act, as amended, 16 U.S.C. § 670 (c)(1).

ADMINISTRATIVE INFORMATION AND ORDER OF PRECEDENCE

This agreement is entered into between the U.S. Army Corps of Engineers, Southwest District, hereinafter referred to as GOVERNMENT, and the organization identified on the Cover Page, block 10a, hereinafter referred to as RECIPIENT. The parties to this agreement act in their independent capacities in their performance of their respective functions under this agreement and neither party is to be considered the officer, agent, or employee of the other.

This agreement will be administered in accordance with, and recipients shall comply with, the applicable requirements of the Office of Management and Budget Grant and Agreement Regulations, Title 2 Code of Federal Regulations (CFR.) Subtitle A, including Title 2 CFR part 200 and the Department of Defense Grants and Agreements Regulations (DoDGAR) 32 CFR Subtitle A, Chapter 1, Subchapter C.

In the event of a conflict between the terms of this agreement and other governing documents, the conflict shall be resolved by giving precedence in descending order as follows:

1. 2 CFR part 200;
2. 32 CFR Subtitle A, Chapter I, Subchapter C (DoDGAR);
3. The articles contained in this agreement;
4. the attachments to this agreement, if any.

MODIFICATIONS TO THIS AGREEMENT:

Modifications to this agreement may be proposed by either party. But neither party shall implement a change until the change has been negotiated and approved by the Government's Grants Officer. The recipient shall submit requests to change the agreement to the Program Manager with a copy to the Grants Officer at least 30 calendar days before the desired effective date. Only the Grants Officer has the authority to act on behalf of the Government to modify this agreement.

Bilateral Modifications: Bilateral modifications may be issued by the Grants Officer for any changes to the Scope of Work, any decrease in funds or increase in funds due to a change in the Scope of Work, and any termination or cancellation of the agreement. Bilateral modifications require the signatures of an authorized representative of the Recipient and the Grants Officer.

Unilateral Modifications: The Government may implement administrative changes to this agreement as a unilateral modification. For the purposes of this agreement, administrative changes include a change in paying office, change in appropriation data, change in phone number of POC, changes in the Grants Officer, points of contact specified for the Federal Government or recipient, changes in address or phone numbers or email addresses, corrections of obvious typographical or calculation errors, or changes that are mutually agreed to by the recipient and the Grants Officer and supported by other documentation. The Grants Officer may also make unilateral changes to exercise pre-negotiated options which do not change the cost or scope of work previously accepted. Unilateral modifications require the signature of the Grants Officer only.

PROCUREMENT: The Recipient's systems for acquiring goods and services under this agreement shall comply with 2 C.F.R. §§ 200.317 to 200.326.

SUBAWARDS: The Recipient shall apply to each subaward the administrative requirements of the DoDGAR applicable to the particular type of sub-recipient. 2 C.F.R. Part 200 shall be applied to awards to universities, hospitals, and other non-profit organizations included in the definition of "recipient" in part 32 of the DoDGAR, as

well as States, local governments, and Indian tribal governments. Unless specifically excluded, provisions below shall apply to sub-recipients performing work under awards.

UNSATISFACTORY PERFORMANCE/NON-COMPLIANCE WITH AWARD PROVISIONS

Failure to perform work in accordance with the terms of the award or failure to comply with any or all of the provisions of the award may result in designation of the Recipient as high risk and assignment of special award conditions or other actions such as withholding payment, requiring performance or financial audits, suspension of award, termination, or any other action provided by law.

TERMINATION: The Grants Officer may terminate this agreement by written notice to the Recipient upon a finding that the Recipient has failed to comply with the material provisions of this agreement. See 2 CFR 200.339. In addition to the remedies identified in 200.339, the Government may use any of the remedies identified in § 200.338 when determined appropriate.

Should the recipient be unable to complete the project, all unexpended monies in addition to any expended amounts determined unallowable in accordance with 2 CFR Part 220 and shall be returned to the U.S. Army Corps of Engineers (USACE).

The USACE SWF District will follow the procedures set forth in 2 CFR 200.341 for providing the opportunity to challenge a suspension or termination action.

The USACE SWF District will follow the procedures set forth in 2 CFR 200.342 for determining the allowability of costs associated with the suspension or termination of an agreement.

CLOSEOUT PROCEDURES: Closeout, subsequent adjustments, continuing responsibilities, and collection of amounts due are subject to the requirements at 2 C.F.R. §§ 200.343, 200.344 and 200.345.

Closeout, adjustment and collection of amounts due shall be accomplished in accordance with 2 CFR 200.343-345 and Subpart F. The Grants Officer may make a settlement for any downward adjustments to the Federal share of costs after closeout reports are received.

Essential documents for closeout include the following:

1. Final SF 270
2. Final SF 425
3. SF 428 with attachment B (C and S when applicable)
4. DD Form 882
5. Final report (See 2 CFR 200.328)
6. Cover Form SF 298

Forms and their instructions can be downloaded at www.grants.gov.

Any additional documents and procedures required by OMB, DOD and the terms and conditions for this agreement will be provided to the cooperator.

The final invoice will only be paid after completion and acceptance of the final reporting package.

Collection of Amounts Due: The USACE SWF District will follow the procedures set forth in 2 CFR 200.345 for the collection of any debt owed to the Federal Government.

OPTIONS: If the agreement contains option(s), the Government reserves the right to exercise pre-negotiated and accepted option(s) unilaterally.

STANDARDS FOR FINANCIAL AND PROGRAM MANAGEMENT

Payments: SEE-2 CFR 200.305

Notice Of Electronic Funds Transfer (EFT): Pursuant to 32 C.F.R. § 22.810, it is a Governmentwide requirement to use EFT in the payment of any grant or cooperative agreement for which an application or proposal was submitted or renewed on or after 26 July 1996, unless the recipient has obtained a waiver by submitting to the head of the pertinent Federal agency a certification that it has neither an account with a financial institution nor an authorized payment agent. To be paid, recipient must submit a Payment Information Form (Standard Form SF-3881) to the responsible DoD payment office.

The Government will reimburse the Recipient up to the negotiated amount for performance in Conformance with the terms of this cost-reimbursable agreement. The Government is not liable for any expenditure in excess of this amount unless agreed to by modification of this agreement. All obligations are subject to the availability of appropriations from Congress.

Payments will be made on a reimbursable basis for allowable, allocable and reasonable actual costs incurred. The recipient shall submit a "Request for Advance or Reimbursement" (SF270) with other required documentation to SWF-CESU-INVOICE@usace.army.mil at minimum on a quarterly basis (within 30 calendar days of the January 1, April 1, July 1, and September 30 reporting periods) and no more frequently than monthly. Invoices shall contain an itemized breakdown of costs either from the financial system or other backup documentation to support the actual costs incurred. Payment will be made by EFT. Ensure an email address is provided in the "Printed Name and Title" block to provide a method of prompt communication should the need arise.

Cost Sharing: If cost sharing has been determined to apply to this Agreement, the Recipient's contributions may count as cost sharing only to the extent that they comply with the criteria at 2 C.F.R. § 200.306

Program Income: SEE-2 CFR 200.307

Recipients are required to account for program income related to projects financed in whole or in part with Federal funds. Program income earned during the project period will be retained by the recipient and shall be added to the funds committed by the sponsoring DoD component and used to further eligible program objectives.

Revision of budget/program plans: Recipient shall request prior approval for plan/budget changes in accordance with 2 C.F.R. § 200.308.

Pre-award Costs are NOT ALLOWED.

No Cost Extension:

If the work being performed under this agreement is severable (i.e. repeated monthly with no final deliverable), the work cannot be extended beyond the awarded period of performance end date. Any work beyond that date must be completed under a new agreement.

If the work being performed under this agreement is non-severable (final deliverable is the goal of the work) the recipient may initiate a one-time extension of the period of performance by up to 12 months unless one or more of the conditions outlined in 1 CFR 200.308 paragraphs (d)(2)(i) through (iii) apply. For one-time extensions, the recipient must notify the Federal awarding agency in writing with the supporting reasons and revised period of performance at least 10 calendar days before the end of the period of performance specified in the Federal award. This one-time extension may not be exercised merely for the purpose of using unobligated balances.

The recipient may not work beyond the period of performance without approval from the Grants Officer and any work performed without approval will not be considered for reimbursement.

Period of Performance Costs: SEE-2 CFR 200.309

A recipient may charge to the Federal award only allowable costs incurred during the period of performance (except as described in § 200.461 Publication and printing costs) and any costs incurred before the Federal awarding agency or pass-through entity made the Federal award that were authorized by the Federal awarding agency of pass-through entity.

Cost Principles: SEE-2 CFR 200 Subpart E

Allowability of costs shall be determined in accordance with the cost principles applicable to the entity incurring the costs. For institutions of higher education that may be recipients, sub-recipients, or contractors the allowability is determined in accordance with the provisions 2 CFR 200 Subpart E – “Cost Principles.”

Financial Management Systems: The Recipient shall establish or use existing financial systems that comply with Generally Accepted Accounting Principles and with 2 C.F.R. §§ 200.302 and 200.303.

Audits: SEE-2 CFR 200 Subpart F

Recipients and sub-recipients that are institutions of higher education or other non-profit organizations (including hospitals) shall be subject to the audit requirements contained in the Single Audit Act Amendments of 1996 (31 U.S.C. 7501-7507) and 2 CFR 200 Subpart F “Audit Requirements.” A copy of the latest audit, if applicable, shall be provided with any proposal. In addition, during performance of any Agreement with the Government, the Recipient shall provide a copy any new auditor’s report to the Government’s Agreement Administrator upon receipt.

Retention and Access to Records: Recipient’s financial records, supporting documents, statistical records and all other records pertinent to this agreement shall be retained and access to these records by the Government shall be permitted in accordance with 2 CFR §200.333 through § 200.337. Copies in electronic format may be substituted for original records.

Financial Reporting: SEE-2 CFR 200. 327

The recipient shall report the status of funds for all projects or programs using SF 270 no later than 30 calendar days after the end of the specified reporting period (quarterly unless specified otherwise in the Statement of Objectives).

A final SF 425 shall be submitted within 90 days after the expiration date of the award.

Financial reports shall be submitted to the Government’s Agreement Administrator at the following email address: SWF-CESU-INVOICE@usace.army.mil

Monitoring and Reporting Program Performance

Recipients shall monitor the program and submit performance reports in accordance with 2 CFR 200.328. Reports may be submitted in electronic form.

The required performance reports identified in the Cooperative Agreement statement of work or statement of objectives prescribes the frequency with which performance reports shall be submitted. Form SF-PPR will be used for reporting and will be submitted electronically to SWF-CESU-INVOICE@usace.army.mil. Unless stated otherwise, performance in the award reports will be due quarterly. The type of information to be contained in the performance report is identified in 2 CFR 200.328. In addition, the report must include the percentage of work completed, and the expected completion of future work. Each comment should be associated with a line item on the agreement.

Any required technical annual reports will be stated within the Statement of Objectives.

FINAL PERFORMANCE REPORTS are due 90 calendar days after the expiration date or termination of the award. Final report needs to have OMB form SF 298.

Property Management:

Equipment: Equipment purchased under the cooperative agreement shall vest with the recipient, and its use, management, and disposition shall be in accordance with 2 C.F.R. § 200.313.

Title to equipment acquired under a Federal award will vest upon acquisition in the non-Federal entity, unless a statute specifically authorized the Federal agency to vest title in the non-Federal entity without further obligation to the Federal Government, and the Federal agency elects to do so, the title must be a conditional title per 2 CFR 200.313(a).

When original or replacement equipment acquired under a Federal award is no longer needed for the original project or program or other activities currently or previously supported by a Federal awarding agency, except as otherwise provided in Federal statutes, regulations or Federal awarding agency disposition instructions, the non-Federal entity must request disposition instructions from the Federal awarding agency if required by the terms and conditions of the Federal award. [For this agreement, the Federal awarding agency requests that any equipment items vital to support military readiness missions be retained by the Federal government.] Items of equipment acquired by the recipient using Federal funds with a current market value of less than \$5,000 shall vest with the recipient subject to conditions of 2 CFR 200.313(e)(1).

Supplies: Title to supplies (including computing devices) will vest in the non-Federal entity upon acquisition subject to conditions in 2 CFR 200.314. If there is a residual inventory of unused supplies exceeding \$5,000 in total aggregate value upon termination or completion of the project or program and the supplies are not needed for any other Federal award, the non-Federal entity must retain the supplies for use on other activities or sell them, but must, in either case, compensate the Federal government for its share.

Intangible Property: Title to intangible property acquired under a Federal award vests upon acquisition in the non-Federal entity subject to conditions in 2 CFR 200.315. DoD reserves a royalty-free, nonexclusive and irrevocable right to reproduce, publish, or otherwise use the work for Federal purposes, and to authorize others to do so.

Rights to Inventions Made under a Contract, Grant or Cooperative Agreement

Cooperative agreements for the performance of experimental, developmental, or research work shall provide for the rights of the Federal Government and the recipient in any resulting invention in accordance with 37 CFR part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms under Government Grants, Contracts and Cooperative Agreements." Any intent to seek patents for any inventions resulting from research conducted using a Department of Defense grant or cooperative agreement must be disclosed on the DD form 882, Report of Inventions and Subcontracts, as described in section 2 CFR 200.315 of this document.

Government Furnished Property: Title to federally owned property remains vested in the Federal Government. Federally furnished equipment is not in-kind assistance. Recipient shall submit an annual inventory report to the Government listing all federally owned property in their custody.

Reporting Requirements: The following forms shall be utilized to meet 2 CFR part 200 reporting requirements:

- SF-428 Tangible Personal Property Report

- SF-428 A – Annual Report due within 30 days after completion of each period of performance

- SF-428 B – Final Report due within 90 days after completion of the award

- SF-428 C – Disposition Request

- RPSR – Real Property Status Report

- RPSR Attachment A – General Reporting

- RPSR Attachment B – Request to Acquire, Improve or Furnish

- RPSR Attachment C – Disposition Request

Procurement Standards: The recipient's procurement system shall comply with the standards identified in part § 200.317 through 326 for use by recipients in establishing procedures for the procurement of supplies and other expendable property, equipment, real property, and other services with Federal Funds. The non-Federal entity must use its own documented procurement procedures which reflect applicable State, local and Tribal laws and regulations, provided that the procurements conform to applicable Federal law and the standards identified in this part.

Claims, Disputes, and Appeals

Parties shall communicate with one another in good faith and in a timely and cooperative manner when raising issues under this Cooperative Agreement. Department of Defense policy is to resolve issues through discussions and mutual agreement at the Grants Officer's level, either through unassisted negotiations or through a mutually agreeable means of Alternative Dispute Resolutions, whenever possible.

When a claim cannot be resolved by the parties, the parties agree to use the procedures identified in 32 C.F.R. § 22.815 as the administrative process to resolve claims, disputes and appeals. Under 32 C.F.R. § 22.815, a recipient's claim must: (1) be submitted in writing; (2) specifying the nature and basis for the relief requested; and (3) include all data that supports the claim. Claims by a DoD component to a recipient shall be the subject of a written decision by a Grants Officer. Within 60 calendar days of receipt of a written claim, the Grants Officer shall either: (1) prepare a written decision; or (2) notify the Recipient of a specific date when he or she will render a written decision if more time is required to do so. The decision of the Grants Officer is final. The recipient has the right to appeal the decision to the Grant Appeal Authority within 90 days of receiving the decision. Particulars concerning the appeal process are specified in Department of Defense Directive 3210.06, 32 C.F.R. § 22.815(e), and Army Appeals Authority AFARS § 5133.90 (Grant and Cooperative Agreement Claims, Disputes and Appeals).

Nothing in this section is intended to limit the recipient's right to any remedy under the law.

Compliance with Laws: By signing or accepting funds under this agreement, Recipient agrees that it will comply with all applicable federal, state and local laws, codes, regulations, rules and orders.

Certification Regarding Lobbying: A separate certification regarding lobbying must be submitted per 32 CFR. Part 28.

Prohibition on Using Funds under Grants and Cooperative Agreements with Entities that Require Certain Internal Confidentiality Agreements: SEE Section 743 of the Financial Services and General Government Appropriations Act, 2015 (Division E of the Consolidated and Further Continuing Appropriations Act, 2015, Pub. L. 113-235)

(a) The recipient may not require its 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) The recipient must notify its employees, contractors, or 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 (a) of this award provision 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 Government determines that the recipient is not in compliance with this award provision, it:

(1) Will prohibit the recipient's use of funds under this award, in accordance with section 743 of Division E of the Consolidated and Further Continuing Resolution Appropriations Act, 2015, (Pub. L. 113-235) or any successor provision of law; and

(2) May pursue other remedies available for the recipient's material failure to comply with award terms and conditions.

2 CFR § 200.216 Prohibition on certain telecommunications and video surveillance services or equipment.

(a) Recipients and sub-recipients are prohibited from obligating or expending loan or grant funds to:

(1) Procure or obtain;

(2) Extend or renew a contract to procure or obtain; or

(3) Enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. As described in Public Law 115-232, section 889, **covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).**

(i) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).

(ii) Telecommunications or video surveillance services provided by such entities or using such equipment.

(iii) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

(b) In implementing the prohibition under Public Law 115-232, section 889, subsection (f), paragraph (1), heads of executive agencies administering loan, grant, or subsidy programs shall prioritize available funding and technical support to assist affected businesses, institutions and organizations as is reasonably necessary for those affected entities to transition from covered communications equipment and services, to procure replacement equipment and services, and to ensure that communications service to users and customers is sustained.

(c) See Public Law 115-232, section 889 for additional information.

(d) See also § 200.471.

2 CFR § 200.471 Telecommunication costs and video surveillance costs.

(a) Costs incurred for telecommunications and video surveillance services or equipment such as phones, internet, video surveillance, cloud servers are allowable except for the following circumstances:

(b) Obliging or expending covered telecommunications and video surveillance services or equipment or services as described in § 200.216 to:

(1) Procure or obtain, extend or renew a contract to procure or obtain;

(2) Enter into a contract (or extend or renew a contract) to procure; or

(3) Obtain the equipment, services, or systems.

32 CFR § 22.815 Claims, disputes, and appeals.

(a) Award terms. Grants officers shall include in grants and cooperative agreements a term or condition that incorporates the procedures of this section for:

(1) Processing recipient claims and disputes.

(2) Deciding appeals of grants officers' decisions.

(b) Submission of claims -

(1) Recipient claims. If a recipient wishes to submit a claim arising out of or relating to a grant or cooperative agreement, the grants officer shall inform the recipient that the claim must:

(i) Be submitted in writing to the grants officer for decision;

(ii) Specify the nature and basis for the relief requested; and

(iii) Include all data that supports the claim.

(2) DoD Component claims. Claims by a DoD Component shall be the subject of a written decision by a grants officer.

(c) Alternative Dispute Resolution (ADR) -

(1) Policy. DoD policy is to try to resolve all issues concerning grants and cooperative agreements by mutual agreement at the grants officer's level. DoD Components therefore are encouraged to use ADR procedures to the

maximum extent practicable. ADR procedures are any voluntary means (e.g., mini-trials or mediation) used to resolve issues in controversy without resorting to formal administrative appeals (see paragraph (e) of this section) or to litigation.

(2) Procedures.

(i) The ADR procedures or techniques to be used may either be agreed upon by the Government and the recipient in advance (e.g., when agreeing on the terms and conditions of the grant or cooperative agreement), or may be agreed upon at the time the parties determine to use ADR procedures.

(ii) If a grants officer and a recipient are not able to resolve an issue through unassisted negotiations, the grants officer shall encourage the recipient to enter into ADR procedures. ADR procedures may be used prior to submission of a recipient's claim or at any time prior to the Grant Appeal Authority's decision on a recipient's appeal (see paragraph (e)(3)(iii) of this section).

d) Grants officer decisions.

(1) Within 60 calendar days of receipt of a written claim, the grants officer shall either:

(i) Prepare a written decision, which shall include the reasons for the decision; shall identify all relevant data on which the decision is based; shall identify the cognizant Grant Appeal Authority and give his or her mailing address; and shall be included in the award file; or

(ii) Notify the recipient of a specific date when he or she will render a written decision, if more time is required to do so. The notice shall inform the recipient of the reason for delaying the decision (e.g., the complexity of the claim, a need for more time to complete ADR procedures, or a need for the recipient to provide additional information to support the claim).

(2) The decision of the grants officer shall be final, unless the recipient decides to appeal. If a recipient decides to appeal a grants officer's decision, the grants officer shall encourage the recipient to enter into ADR procedures, as described in paragraph (c) of this section.

(e) Formal administrative appeals -

(1) Grant appeal authorities. Each DoD Component that awards grants or cooperative agreements shall establish one or more Grant Appeal Authorities to decide formal, administrative appeals in accordance with paragraph (e)(3) of this section. Each Grant Appeal Authority shall be either:

(i) An individual at a grade level in the Senior Executive Service, if civilian, or at the rank of Flag or General Officer, if military; or

(ii) A board chaired by such an individual.

(2) Right of appeal. A recipient has the right to appeal a grants officer's decision to the Grant Appeal Authority (but note that ADR procedures, as described in paragraph (c) of this section, are the preferred means for resolving any appeal).

(3) Appeal procedures -

(i) Notice of appeal. A recipient may appeal a decision of the grants officer within 90 calendar days of receiving that decision, by filing a written notice of appeal to the Grant Appeal Authority and to the grants officer. If a recipient elects to use an ADR procedure, the recipient is permitted an additional 60 calendar days to file the written notice of appeal to the Grant Appeal Authority and grants officer.

(ii) Appeal file. Within 30 calendar days of receiving the notice of appeal, the grants officer shall forward to the Grant Appeal Authority and the recipient the appeal file, which shall include copies of all documents relevant to the

appeal. The recipient may supplement the file with additional documents it deems relevant. Either the grants officer or the recipient may supplement the file with a memorandum in support of its position. The Grant Appeal Authority may request additional information from either the grants officer or the recipient.

(iii) Decision. The appeal shall be decided solely on the basis of the written record unless the Grant Appeal Authority decides to conduct fact-finding procedures or an oral hearing on the appeal. Any fact-finding or hearing shall be conducted using procedures that the Grant Appeal Authority deems appropriate.

(f) Representation. A recipient may be represented by counsel or any other designated representative in any claim, appeal, or ADR proceeding brought pursuant to this section, as long as the representative is not otherwise prohibited by law or regulation from appearing before the DoD Component concerned.

(g) Non-exclusivity of remedies. Nothing in this section is intended to limit a recipient's right to any remedy under the law.

NATIONAL POLICY AWARD PROVISIONS: By signing or accepting funds under this agreement, the recipient assures that it will comply with the applicable provisions of the following national policies (32 CFR Subchapter C)

Nondiscrimination National Policy Requirements

By signing this award or accepting funds under this award, you assure that you will comply with applicable provisions of the national policies prohibiting discrimination:

1. On the basis of race, color, or national origin, in Title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.), as implemented by Department of Defense (DoD) regulations at 32 CFR part 195.
2. On the basis of gender, blindness, or visual impairment, in Title IX of the Education Amendments of 1972 (20 U.S.C. 1681 et seq.), as implemented by DoD regulations at 32 CFR part 196.
3. On the basis of age, in the Age Discrimination Act of 1975 (42 U.S.C. 6101 et seq.), as implemented by Department of Health and Human Services regulations at 45 CFR part 90.
4. On the basis of disability, in the Rehabilitation Act of 1973 (29 U.S.C. 794), as implemented by Department of Justice regulations at 28 CFR part 41 and DoD regulations at 32 CFR part 56.
5. On the basis of disability in the Architectural Barriers Act of 1968 (42 U.S.C. 4151 et seq.) related to physically handicapped persons' ready access to, and use of, buildings and facilities for which Federal funds are used in design, construction, or alteration.

Environmental National Policy Requirements

You must:

1. Comply with all applicable Federal environmental laws and regulations. The laws and regulations identified in this section are not intended to be a complete list.
2. Comply with applicable provisions of the Clean Air Act (42 U.S.C. 7401, et seq.) and Clean Water Act (33 U.S.C. 1251, et seq.).
3. Comply with applicable provisions of the Lead-Based Paint Poisoning Prevention Act (42 U.S.C. 4821-4846), as implemented by the Department of Housing and Urban Development at 24 CFR part 35. The requirements concern lead-based paint in buildings owned by the Federal Government or housing receiving Federal assistance.
4. Immediately identify to us, as the Federal awarding agency, any potential impact that you find this award may have on:
 - a. The quality of the "human environment", as defined in 40 CFR 1508.14, including wetlands; and provide any help we may need to comply with the National Environmental Policy Act (NEPA, at 42 U.S.C. 4321 et seq.), the regulations at 40 CFR 1500-1508, and E.O. 12114, if applicable; and assist us to prepare Environmental Impact Statements or other environmental documentation. In such cases, you may take no action that will have an environmental impact (e.g., physical disturbance of a site such as breaking of ground) or limit the choice of reasonable alternatives to the proposed action until we provide written notification of Federal compliance with NEPA or E.O. 12114.
 - b. Flood-prone areas and provide any help we may need to comply with the National Flood Insurance Act of 1968, as amended by the Flood Disaster Protection Act of 1973 (42 U.S.C. 4001 et seq.), which require flood insurance, when available, for federally assisted construction or acquisition in flood-prone areas.

- c. A land or water use or natural resource of a coastal zone that is part of a federally approved State coastal zone management plan and provide any help we may need to comply with the Coastal Zone Management Act of 1972 (16 U.S.C. 1451, et seq.) including preparation of a Federal agency Coastal Consistency Determination.
- d. Coastal barriers along the Atlantic and Gulf coasts and Great Lakes' shores and provide help we may need to comply with the Coastal Barrier Resources Act (16 U.S.C. 3501 et seq.), concerning preservation of barrier resources.
- e. Any existing or proposed component of the National Wild and Scenic Rivers system and provide any help we may need to comply with the Wild and Scenic Rivers Act of 1968 (16 U.S.C. 1271 et seq.).
- f. Underground sources of drinking water in areas that have an aquifer that is the sole or principal drinking water source and in wellhead protection areas, and provide any help we may need to comply with the Safe Drinking Water Act (42 U.S.C. 300f et seq.).
- 5. Comply fully with the Endangered Species Act of 1973, as amended (ESA, at 16 U.S.C. 1531 et seq.), and implementing regulations of the Departments of the Interior (50 CFR parts 10-24) and Commerce (50 CFR parts 217-227). You also must provide any help we may need in complying with the consultation requirements of ESA section 7 (16 U.S.C. 1536) applicable to Federal agencies or any regulatory authorization we may need based on the award of this grant. This is not in lieu of responsibilities you have to comply with provisions of the Act that apply directly to you as a U.S. entity, independent of receiving this award.
- 6. Fully comply with the Marine Mammal Protection Act of 1972, as amended (MMPA, at 16 U.S.C. 1361 et seq.) and provide any assistance we may need in obtaining any required MMPA permit based on an award of this grant.

National policy requirements concerning live organisms

1. Human subjects.

- a. You must protect the rights and welfare of individuals who participate as human subjects in research under this award and comply with the requirements at 32 CFR part 219, DoD Instruction (DoDI) 3216.02, 10 U.S.C. 980, and when applicable, Food and Drug Administration (FDA) regulations.
- b. You must not begin performance of research involving human subjects, also known as human subjects research (HSR), that is covered under 32 CFR part 219, or that meets exemption criteria under 32 CFR 219.101(b), until you receive a formal notification of approval from a DoD Human Research Protection Official (HRPO). Approval to perform HSR under this award is received after the HRPO has performed a review of your documentation of planned HSR activities and has officially furnished a concurrence with your determination as presented in the documentation.
- c. In order for the HRPO to accomplish this concurrence review, you must provide sufficient documentation to enable his or her assessment as follows:
 - i. If the HSR meets an exemption criterion under 32 CFR 219.101(b), the documentation must include a citation of the exemption category under 32 CFR 219.101(b) and a rationale statement.
 - ii. If your activity is determined as “non-exempt research involving human subjects”, the documentation must include:
 - (A) Assurance of Compliance (i.e., Department of Health and Human Services Office for Human Research Protections (OHRP) Federalwide Assurance (FWA)) appropriate for the scope of work or program plan; and
 - (B) Institutional Review Board (IRB) approval, as well as all documentation reviewed by the IRB to make their determination.
- d. The HRPO retains final judgment on what activities constitute HSR, whether an exempt category applies, whether the risk determination is appropriate, and whether the planned HSR activities comply with the requirements in paragraph 1.a of this section.
- e. You must notify the HRPO immediately of any suspensions or terminations of the Assurance of Compliance.
- f. DoD staff, consultants, and advisory groups may independently review and inspect your research and research procedures involving human subjects and, based on such findings, DoD may prohibit research that presents unacceptable hazards or otherwise fails to comply with DoD requirements.
- g. Definitions for terms used in paragraph 1 of this article are found in DoDI 3216.02.

2. Animals.

- a. Prior to initiating any animal work under the award, you must:
 - i. Register your research, development, test, and evaluation or training facility with the Secretary of Agriculture in accordance with 7 U.S.C. 2136 and 9 CFR 2.30, unless otherwise exempt from this requirement by meeting the conditions in 7 U.S.C. 2136 and 9 CFR parts 1-4 for the duration of the activity.
 - ii. Have your proposed animal use approved in accordance with DoDI 3216.01, Use of Animals in DoD Programs by a DoD Component Headquarters Oversight Office.

- iii. Furnish evidence of such registration and approval to the grants officer.
 - b. You must make the animals on which the research is being conducted, and all premises, facilities, vehicles, equipment, and records that support animal care and use available during business hours and at other times mutually agreeable to you, the United States Department of Agriculture Office of Animal and Plant Health Inspection Service (USDA/APHIS) representative, personnel representing the DoD component oversight offices, as well as the grants officer, to ascertain that you are compliant with 7 U.S.C. 2131 et seq., 9 CFR parts 1-4, and DoDI 3216.01.
 - c. Your care and use of animals must conform with the pertinent laws of the United States, regulations of the Department of Agriculture, and regulations, policies, and procedures of the Department of Defense (see 7 U.S.C. 2131 et seq., 9 CFR parts 1-4, and DoDI 3216.01).
 - d. You must acquire animals in accordance with DoDI 3216.01.
3. Use of Remedies.

Failure to comply with the applicable requirements in paragraphs 1-2 of this section 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. See OAR Article III.

Other National Policy Requirements

1. **Debarment and suspension.** You must comply with requirements regarding debarment and suspension in Subpart C of 2 CFR part 180, as adopted by DoD at 2 CFR part 1125. This includes requirements concerning your principals under this award, as well as requirements concerning your procurement transactions and subawards that are implemented in PROC Articles I through III and SUB Article II.
2. **Drug-free workplace.** You must comply with drug-free workplace requirements in Subpart B of 2 CFR part 26, which is the DoD implementation of 41 U.S.C. chapter 81, "Drug-Free Workplace."
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.
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.
5. **Hatch Act.** If applicable, you must comply with the provisions of the Hatch Act (5 U.S.C. 1501-1508) concerning political activities of certain State and local government employees, as implemented by the Office of Personnel Management at 5 CFR part 151, which limits political activity of employees or officers of State or local governments whose employment is connected to an activity financed in whole or part with Federal funds.
6. **Native American graves protection and repatriation.** If you control or possess Native American remains and associated funerary objects, you must comply with the requirements of 43 CFR part 10, the Department of the Interior implementation of the Native American Graves Protection and Repatriation Act of 1990 (25 U.S.C., chapter 32).
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.
8. **Use of United States-flag vessels.** You must comply with the following requirements of the Department of Transportation at 46 CFR 381.7, in regulations implementing the Cargo Preference Act of 1954:
 - a. Pursuant to Public Law 83-664 (46 U.S.C. 55305), at least 50 percent of any equipment, materials or commodities procured, contracted for or otherwise obtained with funds under this award, and which may be transported by ocean vessel, must be transported on privately owned United States-flag commercial vessels, if available.

b. Within 20 days following the date of loading for shipments originating within the United States or within 30 working days following the date of loading for shipments originating outside the United States, a legible copy of a rated, "on-board" commercial ocean bill-of-lading in English for each shipment of cargo described in paragraph 8.a of this section must be furnished to both our award administrator (through you in the case of your contractor's bill-of-lading) and to the Division of National Cargo, Office of Market Development, Maritime Administration, Washington, DC 20590.

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 website: <https://www.federalregister.gov/documents/2000/12/06/00-30852/executive-office-of-the-president-federal-policy-on-research-misconduct-preamble-for-research>).

10. Requirements for an Institution of Higher Education Concerning Military Recruiters and Reserve Officers Training Corps (ROTC).

a. As a condition for receiving funds available to the DoD under this award, you agree that you are not an institution of higher education (as defined in 32 CFR part 216) that has a policy or practice that either prohibits, or in effect prevents:

i. The Secretary of a Military Department from maintaining, establishing, or operating a unit of the Senior Reserve Officers Training Corps (ROTC) - in accordance with 10 U.S.C. 654 and other applicable Federal laws - at that institution (or any subelement of that institution);

ii. Any student at that institution (or any subelement of that institution) from enrolling in a unit of the Senior ROTC at another institution of higher education.

iii. The Secretary of a Military Department or Secretary of Homeland Security from gaining access to campuses, or access to students (who are 17 years of age or older) on campuses, for purposes of military recruiting in a manner that is at least equal in quality and scope to the access to campuses and to students that is provided to any other employer; or

iv. Access by military recruiters for purposes of military recruiting to the names of students (who are 17 years of age or older and enrolled at that institution or any subelement of that institution); their addresses, telephone listings, dates and places of birth, levels of education, academic majors, and degrees received; and the most recent educational institutions in which they were enrolled.

b. If you are determined, using the procedures in 32 CFR part 216, to be such an institution of higher education during the period of performance of this award, we:

i. Will cease all payments to you of DoD funds under this award and all other DoD grants and cooperative agreements; and

ii. May suspend or terminate those awards unilaterally for material failure to comply with the award terms and conditions.

11. Historic preservation. You must identify to us any:

a. Property listed or eligible for listing on the National Register of Historic Places that will be affected by this award, and provide any help we may need, with respect to this award, to comply with Section 106 of the National Historic Preservation Act of 1966 (54 U.S.C. 306108), as implemented by the Advisory Council on Historic Preservation regulations at 36 CFR part 800 and Executive Order 11593, "Identification and Protection of Historic Properties," [3 CFR, 1971-1975 Comp., p. 559]. Impacts to historical properties are included in the definition of "human environment" that require impact assessment under NEPA (See NP Article II, Section A).

b. Potential under this award for irreparable loss or destruction of significant scientific, prehistorical, historical, or archeological data, and provide any help we may need, with respect to this award, to comply with the Archaeological and Historic Preservation Act of 1974 (54 U.S.C. chapter 3125).

12. Relocation and real property acquisition. You must comply with applicable provisions of 49 CFR part 24, which implements the Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970 (42 U.S.C. 4601, et seq.) and provides for fair and equitable treatment of persons displaced by federally assisted programs or persons whose property is acquired as a result of such programs.

13. Confidentiality of patient records. You must keep confidential any records that you maintain of the identity, diagnosis, prognosis, or treatment of any patient in connection with any program or activity relating to substance abuse education, prevention, training, treatment, or rehabilitation that is assisted directly or indirectly under this award, in accordance with 42 U.S.C. 290dd-2.

14. Pro-Children Act.

You must comply with applicable restrictions in the Pro-Children Act of 1994 (Title 20, Chapter 68, subchapter X, Part B of the U.S. Code) on smoking in any indoor facility:

- a. Constructed, operated, or maintained under this award and used for routine or regular provision of kindergarten, elementary, or secondary education or library services to children under the age of 18.
- b. Owned, leased, or contracted for and used under this award for the routine provision of federally funded health care, day care, or early childhood development (Head Start) services to children under the age of 18.

15. **Constitution Day.** You must comply with Public Law 108-447, Div. J, Title I, Sec. 111 (36 U.S.C. 106 note), which requires each educational institution receiving Federal funds in a Federal fiscal year to hold an educational program on the United States Constitution on September 17th during that year for the students served by the educational institution.

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.

17. **Whistleblower protections.** You must comply with 10 U.S.C. 2409, including the:

- a. Prohibition on reprisals against employees disclosing certain types of information to specified persons or bodies; and
- b. Requirement to notify your employees in writing, in the predominant native language of the workforce, of their rights and protections under that statute.

LIABILITY PROVISION (INDEMNIFICATION)

Governmental Parties:

(1) The Federal Agencies (excluding the U.S. Forest Service), Host University, and Partner Institutions which are governmental parties, each accept responsibility for any property damage, injury, or death caused by the acts or omissions of their respective employees, acting within the scope of their employment, to the fullest extent permitted by their respective applicable laws, including laws concerning self-insurance.

(2) To the extent work by governmental parties is to be performed through sub-contract by non-governmental entities or persons, the governmental party sub-contracting work will require that subcontracted entity or person to meet provisions (1), (2), and (3) for non-governmental parties stated below.

(3) This provision is applicable to the U.S. Forest Service acting by and through the Forest Service, USDA does hereby recognize potential liability for payment of claims for injury or loss of property of personal injury or death caused by the Government, or any officer, agent or employee thereof, while acting within the scope of his/her office of employment under circumstances when the United States, if a private person, would be liable to the claimant in accordance with the law of the place where the act or omission occurred (28 U.S.C. §§1346 (b), 2672 et seq.).

Non-governmental Parties: Work provided by non-governmental entities or persons, will require that entity or person to:

(1) Have public and employee liability insurance from a responsible company or companies with a minimum limitation of one million dollars (\$1,000,000) per person for any one claim, and an aggregate limitation of three million dollars (\$3,000,000) for any number of claims arising from any one incident. In subsequent modifications, the parties may negotiate different levels of liability coverage, as appropriate. The policies shall name the United States as an additional insured, shall specify that the insured shall have no right of subrogation against the United States for payments of any premiums or deductibles due thereunder, and shall specify that the insurance shall be assumed by, be for the account of, and be at the insured's sole risk; and

(2) Pay the United States the full value for all damages to the lands or other property of the United States caused by such person or organization, its representatives, or employees; and

(3) Indemnify, save and hold harmless, and defend the United States against all fines, claims, damages, losses, judgments, and expenses arising out of, or from, any omission or activity of such person or organization, its representatives, or employees.

(4) Non-governmental Partner Institutions shall provide the Federal Agencies confirmation of such insurance coverage, prior to beginning specific work authorized herein and specified in subsequent modifications.

Safeguarding Covered Defense Information and Cyber Incident Reporting (Dec 2019)

(a) *Definitions.* As used in this clause—

“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 contractor(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 contractor 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 contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

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

“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 contractor 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, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data—

Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. 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.

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

(1) For covered contractor 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 clause 252.239-7010, Cloud Computing Services, of this contract.

(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 contract.

(2) For covered contractor 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 clause, the covered contractor 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” (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 Contracting Officer.

(ii)(A) The Recipient shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Recipient shall notify the DoD Chief Information Officer (CIO), via email at osd.dibesia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting 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 contractor’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 Contracting Officer when requesting its recognition under this contract.

(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 contract, 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 clause 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 clause, 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 contract that are designated as operationally critical support and identified in the contract, 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 contractor 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 clause, the Recipient or 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 subcontractors 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 Contracting Officer. Do not send the malicious software to the Contracting 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 clause 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 Contracting Officer will request that the recipient provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) *DoD safeguarding and use of contractor 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 clause that includes contractor 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 contractor 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 contractor (or derived from information obtained from the contractor) under this clause 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 recipient that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) *Use and release of recent attributional/proprietary information created by or for DoD.* Information that is obtained from the recipient (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, 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 clause 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 clause 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 clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) *Subcontracts.* The Recipient shall—

(1) Include this term, including this 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 recipient shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

(i) Notify the agreement recipient (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the agreement recipient (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

(a) *Definitions.*

Basic Assessment” means a recipient’s self-assessment of the recipient 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” 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 agreement and provided to the recipient by or on behalf of DoD in support of the performance of the agreement; or
- (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the recipient in support of the performance of the agreement.

“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’ 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 term 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.

(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/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html, if necessary.

(d) *Procedures.* Summary level scores for all assessments will be posted in the **Supplier Performance Risk System (SPRS)** (<https://www.sprs.csd.disa.mil/>) 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 <mailto:webptsmh@navy.mil> 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 contract—

(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 Codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total Score	Date score of 110 will be 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 term. 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) Subcontracts.

(1) The Recipient shall insert the substance of this term, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items).

(2) The Recipient shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, unless the 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/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html, 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 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 request for proposal) posted in SPRS, the subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800-171 DoD Assessment Methodology, to <mailto:webpmsmh@navy.mil> for posting to SPRS along with the information required by paragraph (d) of this term.

END OF TERMS & CONDITIONS