**General Services Administration**

Federal Acquisition Service

Technology Transformation Services

18F and Office of Acquisition

1800 F Street NW | Washington, DC | 20405

Office of Head Start Training and Technical Assistance Data Platform

Appendix 1

**Contract Terms and Conditions**

# Transparency Policy & Security Requirements

Contractors are advised that TTS reserves the right to publish documents associated with this requirement on a publicly-available website, including any Requests for Quotation (including amendments), Question and Answer exchanges with contractors (source-identifying information removed), and other relevant information that is not confidential or proprietary in nature or source selection sensitive information that would otherwise implicate procurement integrity concerns.

Upon award, TTS may publish the total awarded price and certain non-source-identifying data (for example, the number of bids, the mean price, median, and standard deviation of price). During the performance of this task order, TTS may similarly publish data related to project management (for example, user stories, milestones, and performance metrics) and top-line spending data.

* 1. **Section 508 Compliance**

The following Section 508 accessibility standards apply to the work to be performed.

1. Section 508 of the Rehabilitation Act of 1973

In 1998, Congress amended the Rehabilitation Act of 1973 to require Federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities. The law (29 U.S.C § 794 (d)) applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Under Section 508, agencies must give disabled employees and members of the public access to information comparable to the access available to others.

The U.S. Access Board is responsible for developing Information and Communication Technology (ICT) accessibility standards to incorporate into regulations that govern Federal procurement practices. On January 18, 2017, the Access Board issued a final rule that updated accessibility requirements covered by Section 508, and refreshed guidelines for telecommunications equipment subject to Section 255 of the Communications Act. The final rule went into effect on January 18, 2018.

The rule updated and reorganized the Section 508 Standards and Section 255 Guidelines in response to market trends and innovations in technology. The refresh also harmonized these requirements with other guidelines and standards both in the U.S. and abroad, including standards issued by the European Commission, and with the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG 2.0), a globally recognized voluntary consensus standard for web content and ICT.

https://www.section508.gov/manage/laws-and-policies

The Architectural and Transportation Barriers Compliance Board (Access Board issued final guidelines for accessibility, usability, and compatibility of telecommunications equipment and customer premises equipment covered by section 255 of the Telecommunications Act of 1996. Section 255 of the Communications Act, as amended by the Telecommunications Act of 1996, requires telecommunications products and services to be accessible to people with disabilities. Manufacturers must ensure that products are “designed, developed, and fabricated to be accessible to and usable by individuals with disabilities” when it is readily achievable to do so. Accessibility guidelines issued by the Board under Section 255 address the telecommunications products covered including wired and wireless telecommunication devices such as:

* telephones (including pay phones and cellular phones),
* pagers,
* fax machines,
* other products that have a telecommunication service capability, such as computers with modems and,
* Equipment that carriers use to provide services, such as a phone company’s switching equipment.

https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-telecommunications-act-guidelines

1. Functional Performance Criteria

Section 1194.31 Functional Performance Criteria

This section provides functional performance criteria for overall product evaluation and for technologies or components for which there is no specific requirement under other sections. These criteria are also intended to ensure that the individual accessible components work together to create an accessible product. This section requires that all product functions, including operation and information retrieval, be operable through at least one mode addressed in each of the paragraphs. Go to Sub-part C Functional Performance Criteria 1194.31 at:

<https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards#subpart_c>

1. FAR Part 39 - Acquisition of Information Technology

### 39.000 -- Scope of Part.

This part prescribes acquisition policies and procedures for use in acquiring—

(a) Information technology, including financial management systems, consistent with other parts of this regulation, OMB Circular No. A-127, Financial Management Systems and OMB Circular No. A-130, Management of Federal Information Resources; and

(b) Information and information technology.

### 39.001 -- Applicability.

This part applies to the acquisition of information technology by or for the use of agencies except for acquisitions of information technology for national security systems.

### 39.002 -- Definitions.

As used in this part--

“Modular contracting” means use of one or more contracts to acquire information technology systems in successive, interoperable increments.

1. 39.104 – Information Technology Services.

When acquiring information technology services, solicitations must not describe any minimum experience or educational requirement for proposed contractor personnel unless the contracting officer determines that the needs of the agency—

(a) Cannot be met without that requirement; or

(b) Require the use of other than a performance-based acquisition (see [Subpart 37.6](http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/37.htm#P236_36578)).

### 39.106 -- Contract Clause.

The contracting officer shall insert a clause substantially the same as the clause at [52.239-1](http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/52_237.htm#P114_19100), Privacy or Security Safeguards, in solicitations and contracts for information technology which require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services.

### 39.201 Scope of subpart.

(a) This subpart implements section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR part 1194).

(b) Further information on section 508 is available via the Internet at [http://www.section508.gov](http://www.section508.gov/).

(c) When acquiring EIT, agencies must ensure that--

(1) Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities; and

(2) Members of the public with disabilities seeking information or services from an agency have access to and use of information and data that is comparable to the access to and use of information and data by members of the public who are not individuals with disabilities.

### 39.202 Definition.

Undue burden, as used in this subpart, means a significant difficulty or expense.

1. 39.203 Applicability.

(a) Unless an exception at [39.204](http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/39.htm#P77_13036) applies, acquisitions of EIT supplies and services must meet the applicable accessibility standards at 36 CFR part 1194.

(b)

(1) Exception determinations are required prior to contract award, except for indefinite-quantity contracts (see paragraph (b)(2) of this section).

(2) Exception determinations are not required prior to award of indefinite-quantity contracts, except for requirements that are to be satisfied by initial award. Contracting offices that award indefinite-quantity contracts must indicate to requiring and ordering activities which supplies and services the contractor indicates as compliant and show where full details of compliance can be found (*e.g.,* vendor's or other exact website location).

(3) Requiring and ordering activities must ensure supplies or services meet the applicable accessibility standards at 36 CFR part 1194, unless an exception applies, at the time of issuance of task or delivery orders. Accordingly, indefinite-quantity contracts may include noncompliant items; however, any task or delivery order issued for noncompliant items must meet an applicable exception.

(c)

(1) When acquiring commercial items, an agency must comply with those accessibility standards that can be met with supplies or services that are available in the commercial marketplace in time to meet the agency's delivery requirements.

(2) The requiring official must document in writing the no availability, including a description of market research performed and which standards cannot be met, and provide documentation to the contracting officer for inclusion in the contract file.

### 39.204 Exceptions.

The requirements in [39.203](http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/39.htm#P68_11391) do not apply to EIT that--

(a) Is purchased in accordance with [Subpart 13.2](http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/13.htm#P196_27888) (micro-purchases) prior to April 1, 2005. However, for micro-purchases, contracting officers and other individuals designated in accordance with [1.603-3](http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/01.htm#P1019_50735) are strongly encouraged to comply with the applicable accessibility standards to the maximum extent practicable;

(b) Is for a national security system;

(c) Is acquired by a contractor incidental to a contract;

(d) Is located in spaces frequented only by service personnel for maintenance, repair or occasional monitoring of equipment; or

(e) Would impose an undue burden on the agency.

(1) *Basis*. In determining whether compliance with all or part of the applicable accessibility standards in 36 CFR part 1194 would be an undue burden, an agency must consider--

(i) The difficulty or expense of compliance; and

(ii) Agency resources available to its program or component for which the supply or service is being acquired.

(2) *Documentation.*

(i) The requiring official must document in writing the basis for an undue burden decision and provide the documentation to the contracting officer for inclusion in the contract file.

(ii) When acquiring commercial items, an undue burden determination is not required to address individual standards that cannot be met with supplies or service available in the commercial marketplace in time to meet the agency delivery requirements (see [39.203](http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/39.htm#P68_11391)(c)(2) regarding documentation of nonavailability). <http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/39.htm>

1. Provisions and Clauses:

When purchasing consulting services and labor hours to provide development, authoring, testing, installation, configuration, maintenance, training, and other consulting services related to ICT, the Contractors shall ensure the personnel providing the labor hours possess the knowledge, skills, and ability necessary to address the applicable Revised 508 Standards defined in this contract and shall provide supporting documentation upon request.

When the Contractors provides custom ICT development services pursuant to this contract, the Contractors shall ensure the ICT fully conforms to the applicable Revised 508 Standards prior to delivery and before final acceptance.

1. Installation, Configuration & Integration Services

When the Contractors provides installation, configuration or integration services for equipment and software pursuant to this contract, the Contractors shall not install, configure or integrate the equipment and software in a way that reduces the level of conformance with the applicable Revised 508 Standards.

The Contractors shall ensure maintenance upgrades, substitutions, and replacements to equipment and software pursuant to this contract do not reduce the original level of conformance with the applicable Revised 508 Standards at the time of contract award.

The contractor shall test and validate the ICT solution for conformance to the Revised 508 Standards, in accordance with the agency required testing methods.

* Contractors shall validate conformance to the applicable Revised 508 Standards using a defined testing process. The Contractors must describe test process and provide the testing results to the agency. The testing shall include type of Assistive Technology (AT) and automatic tools used for validating testing.

The Contractors shall maintain and retain full documentation of the measures taken to ensure compliance with the applicable requirements, including records of any testing or demonstrations conducted. Before acceptance, the contractor shall provide an **Accessibility Conformance Report (ACR)** for each ICT item that is developed, updated, configured for the agency, and when product substitutions are offered. The ACR should be based on the latest version of the Voluntary Product Accessibility Template (VPAT)).

To be considered for award, an ACR must be submitted for each ICT Item, and must be completed according to the instructions provided by ITIC.

Before acceptance, when the contractor is required to perform testing to validate conformance to the agency's accessibility requirements, the vendor shall provide a **Supplemental Accessibility Conformance Report (SAR)** that contains the following information:

* Accessibility test results based on the required test methods.
* Documentation of features provided to help achieve accessibility and usability for people with disabilities.
* Documentation of core functions that cannot be accessed by persons with disabilities.
* Documentation on how to configure and install the ICT item to support accessibility.
* When an ICT item is an authoring tool that generates content (including documents, reports, videos, multimedia productions, web content, etc).

Before final acceptance of any ICT item, including updates and replacements, if the Contractors claims its products or services satisfy the applicable Revised 508 Standards specified in the statement of work, and the contracting officer determines that any furnished ICT item is not in compliance with such requirements, the contracting officer will promptly inform the Contractors in writing of the noncompliance. The Contractors shall, at no cost to the agency, repair or replace the non-compliant products or services within the period specified by the contracting officer.

1. Revised 508 Standards, Safe Harbor and FAR Update

Federal agencies have been working to transition to the [Revised 508 Standards](https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule), which aim to make information technology more accessible to all users, and bring U.S. accessibility standards in line with international standards. The FAR Council is also working on regulatory updates to the Federal Acquisition Regulation (FAR), and as of January 18, 2018, agencies should proactively address the requirements of the Revised 508 Standards in their procurement processes. Note that all new or revised information and communication technology (ICT) must satisfy the Revised 508 Standards, but older ICT (previously referred to as Electronic and Information Technology (EIT)), providing that it was compliant with the Original 508 Standards, may fall under a “safe harbor” provision.

* **Safe Harbor** - The Revised 508 Standards also include a “safe harbor” provision for existing (i.e., legacy) ICT. Under this safe harbor, unaltered, **existing ICT (including electronic content) that complies with the Original 508 Standards need not be modified or upgraded to conform to the Revised 508 Standards.**
  + This safe harbor applies on an element-by-element basis to each component or portion of the existing ICT, with each component or portion assessed separately.
  + **Existing, unaltered ICT that did not comply with the Original 508 Standards as of January 18, 2018 must now be brought into compliance with the Revised 508 Standards. Please visit** [**https://www.section508.gov/blog/Revised-508-Standards-Safe-Harbor-and-FAR-Update**](https://www.section508.gov/blog/Revised-508-Standards-Safe-Harbor-and-FAR-Update)

According to the Section 508 standards, part 1194.2, “(b) When procuring a product, agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation.  Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards.  If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards.”

1. Contract Staff and Vendors

Misrepresentation of Section 508 compliance or failure to provide ICT products or services that meet the proposed and accepted level of conformance is unacceptable. They may result in termination for cause or other actions as specified in the HHSAR or FAR.

1. In order to facilitate the Government’s determination whether proposed EIT supplies meet applicable Section 508 accessibility standards, offeror must submit an HHS Section 508 Product Assessment Template, in accordance with its completion instructions. The purpose of the template is to assist HHS acquisition and program officials in determining whether proposed EIT supplies conform to applicable Section 508 accessibility standards. The template allows offeror or developers to self-evaluate their supplies and document—in detail—whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available under Section 508 policy. (See HHS PAT Link below.

To determine whether proposed EIT services meet applicable Section 508 accessibility standards, offeror must provide enough information to assist the Government in determining that the EIT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.

1. In the event of a modification(s) to this contract or order, which adds new EIT supplies or services or revises the type of, or specifications for, supplies or services, the Contracting Officer may require that the contractor submit a completed HHS Section 508 Product Assessment Template and any other additional information necessary to assist the Government in determining that the EIT supplies or services conform to Section 508 accessibility standards. Instructions for documenting accessibility via the HHS Section 508 Product Assessment Template may be found under Section 508 policy on the HHS website: ([http://www.hhs.gov/web/508](https://www.hhs.gov/web/508)). If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.
2. The leaderboard below demonstrates how compliant our websites are with Section 508. The accessibility of websites for each Operating Division is determined each month by an automated scan of every page of every website.
3. Scores: Acceptable- 76% and above. Needs Improvement- 75.99% and below.
4. Deliverables: Schedule for Contractor Submission of Section 508 Annual Report, Annually at the start of each option.

In addition to Section 508 requirements, HHS has policies, standards, and requirements for electronic documents that include but aren’t limited to the following:

* Document file name should not contain any spaces or special characters.
* Document file name needs to be concise, generally limited to 20-30 characters and should clarify the contents of the file.
* All Document properties should be filled out Title, Author, (an HHS OpDiv, StaffDiv, or Program Office---not an individual’s names) Subject, and Keywords
* Use electronic version for any signatures (see <http://webstandards.hhs.gov/standards/41>)
* Use Exit Icon disclaimer for all non-government sites

## Privacy Act

Performance of this Task Order may require that personnel have access to privacy information. Contractor personnel shall adhere to the privacy act, Title 5 of the U.S. Code, Section 552a and any other applicable applicable rules and regulations.

## Protection of Information

The Contractor shall be responsible for properly protecting all information used, gathered, disclosed, or developed as a result of work under this Task Order. The Contractor shall also protect all Government data by treating information as sensitive. All information gathered or created under this Task Order shall be considered as Sensitive but Unclassified (SBU) information. The use of this data is subject to the privacy act and shall be utilized in full accordance with all rules of conduct as applicable to privacy act Information.

## Organizational Conflicts of Interest

The prospective Contractor certifies, to the best of its knowledge and belief, that it is not aware of any information bearing on the existence of any potential organizational conflict of interest.

If the prospective Contractor cannot so certify, it shall provide a disclosure statement in its proposal which describes all relevant information concerning any past, present, or planned interests bearing on whether it (including its chief executives and directors, or any proposed consultant or subcontractor) may have a potential organizational conflict of interest.

Prospective Contractors should refer to FAR Subpart 9.5 and GSAM Part 509 for policies and procedures for avoiding, neutralizing, or mitigating organizational conflicts of interest.

If the Contracting Officer determines that a potential conflict exists, the prospective Contractor shall not receive an award unless the conflict can be avoided or otherwise resolved through the inclusion of a special contract clause or other appropriate means. The terms of any special clause are subject to negotiation.

## Data Rights and Ownership of Deliverables

*Data Rights and Ownership of Deliverables* – OHS intends that all software and documentation delivered by the Contractor will be made publicly available without restriction. This software and documentation includes, but is not limited to, data, documents, graphics, code, plans, reports, schedules, schemas, metadata, architecture designs, and the like; all new open source software created by the Contractor and forks or branches of current open source software where the Contractor has made a modification; and all new tooling, scripting configuration management, infrastructure as code, or any other final changes or edits to successfully deploy or operate the software. Contractor’s should not be using any pre-existing commercial code unless it is provided by the Government. For the avoidance of doubt, the foregoing is included in the definition of "data" set forth in the FAR clause at 52.227-17, incorporated into this contract.

To the extent that the Contractor seeks to incorporate into the software delivered under this task order any software that was not first produced in the performance of this task order, OHS encourages the Contractor to incorporate either software that is in the public domain, or free and open source software that qualifies under the Open Source Definition promulgated by the Open Source Initiative. In any event, the Contractor must promptly disclose to OHS in writing, and list in the documentation, any software incorporated in the delivered software that is subject to a license fee.

If software delivered by the Contractor incorporates software that is subject to an open source license that provides implementation guidance, then the Contractor must ensure compliance with that guidance. If software delivered by the Contractor incorporates software that is subject to an open source license that does not provide implementation guidance, then the Contractor must attach or include the terms of the license within the work itself, such as in code comments at the beginning of a file, or in a license file within a software repository.

The Government data rights of software deliverables and all other data first produced in the performance of this task order shall be in accordance with **FAR 52.227-17 Rights in Data -- Special Works**. The Government may require the contractor to assign its copyright in such data to the Government in accordance with **FAR 52.227-17(c)(1)(ii)** or to publicly post it with an appropriate notice.

Ownership of code repositories furnished as Government-Furnished Information (GFI) and Government-provided data entered into any and all systems, system documentation, and other related system information shall reside with the Government.

## Personnel Security Requirements

The Contractor (and/or any subcontractor) and its employees shall comply with Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors; OMB M-05-24; FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors; HHS HSPD-12 policy; and Executive Order 13467, Part 1 §1.2.

The Contractor (and/or any subcontractor) and its employees shall comply with computing and security standards including:

* Federal Information Security Management Act (FISMA) as part of the e-government Act of 2002
* Homeland Security Presidential Directive (HSPD)-12,
* Policy for a Common Identification Standard for Federal Employees and Contractors;
* Office of Management and Budget (OMB) Memorandum (M)05-24;
* Federal Information Processing Standards Publication (FIPS PUB) Number 201,
* FAR Subpart 4.13,
* FAR 52.204-9, and
* HHS HSPD-12 policy

The Contractor shall refer to the HHS-OCIO Policy for Information Systems Security and Privacy, dated July 7, 2011. The Contractor shall become familiar with the HHS Departmental Information Security Policies, which may be found at https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/index.html. The HHS Cybersecurity Program develops policies, procedures, and guidance to serve as a foundation for the HHS information security program. These documents implement relevant Federal laws, regulations, standards, and guidelines that provide a basis for the information security program at the Department. The Contractor must become familiar with HHS Cybersecurity Program guidelines as presented at https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/information-security-privacy-program/index.html.

## IT Security Requirements

A. Baseline Security Requirements

1) Applicability. The requirements herein apply whether the entire contract or order (hereafter “contract”), or portion thereof, includes either or both of the following:

a. Access (Physical or Logical) to Government Information: A Contractor (and/or any subcontractor) employee will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information as required to perform their work. Access is contingent upon positive adjudication of background check.

b. Operate a Federal System Containing Information: A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that supports the OHS mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of “information technology” (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

2) Safeguarding Information and Information Systems. In accordance with the Federal Information Processing Standards Publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, the Contractor (and/or any subcontractor) shall:

a. Protect government information and information systems in order to ensure:

* Confidentiality, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
* Integrity, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
* Availability, which means ensuring timely and reliable access to and use of information.

b. Provide security for any Contractor systems, and information contained therein, connected to an HHS network or operated by the Contractor on behalf of OHS regardless of location.

c. Adopt and implement the policies, procedures, controls, and standards required by the HHS Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract.

d. Comply with the Privacy Act requirements.

3) Information Security Categorization. In accordance with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, Appendix C, and based on information provided by the ISSO, CISO, or other security representative, the contractor shall work with the OHS security team to categorize information or information systems. The categorization can change at any time throughout the lifecycle of the system. The contractor shall ensure proper controls are implemented based on the categorization.

4) Controlled Unclassified Information (CUI). CUI is defined as “information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information.” The Contractor (and/or any subcontractor) must comply with Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR, part 2002) when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term “handling” refers to “…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, reusing, and disposing of the information.” 81 Fed. Reg. 63323. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, shall be:

a. marked appropriately;

b. disclosed to authorized personnel on a Need-To-Know basis;

c. protected in accordance with NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations if handled by internal Contractor system; and

d. returned to OHS control, destroyed when no longer needed, or held until otherwise directed. Destruction of information and/or data shall be accomplished in accordance with NIST SP 800-88, Guidelines for Media Sanitization.

5) Protection of Sensitive Information. For security purposes, information is or may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect all government information that is or may be sensitive in accordance with OMB Memorandum M-06-16, Protection of Sensitive Agency Information by securing it with a FIPS 140-2 validated solution.

6) Confidentiality and Nondisclosure of Information. Any information provided to the contractor (and/or any subcontractor) by OHS or collected by the contractor on behalf of OHS shall be used only for the purpose of carrying out the provisions of this contract and shall not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its employees and subcontractors shall be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any OHS records may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.

The confidentiality, integrity, and availability of such information shall be protected in accordance with HHS and OHS policies. Unauthorized disclosure of information will be subject to the HHS/OHS sanction policies and/or governed by the following laws and regulations without limitation:

a. 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);

b. 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and

c. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).

7) Internet Protocol Version 6 (IPv6). All procurements using Internet Protocol shall comply with OMB Memorandum M-05-22, Transition Planning for Internet Protocol Version 6 (IPv6).

8) Websites and Digital Services. All new and existing public-facing government websites shall comply with the Integrated Digital Experience Act (IDEA).

9) Government Websites. All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.

10) Contract Documentation. The Contractor shall use provided templates, policies, forms and other agency documents, if applicable, to comply with contract deliverables as appropriate.

11) Standard for Encryption. The Contractor (and/or any subcontractor) shall:

a. Comply with the HHS Standard for Encryption of Computing Devices and Information to prevent unauthorized access to government information.

b. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with FIPS 140-2 validated encryption solution.

c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and OHS-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).

d. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the contracting officer’s representative (COR) prior to implementation of the solution.

e. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to the COR upon request and at the conclusion of the contract.

12) Contractor Non-Disclosure Agreement (NDA). Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract shall complete the OHS non-disclosure agreement. A copy of each signed and witnessed NDA shall be submitted to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.

13) Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA). When applicable, the Contractor shall assist the OHS Senior Official for Privacy (SOP) or designee with conducting a PTA for the information system and/or information handled under this contract to determine whether or not a full PIA needs to be completed.

a. If the results of the PTA show that a full PIA is needed, the Contractor shall assist the OHS SOP or designee with completing a PIA for the system or information within 30 days after completion of the PTA and in accordance with HHS policy and OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

b. The Contractor shall assist the OHS SOP or designee in reviewing the PIA at least every three years throughout the system development lifecycle (SDLC) / information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.

B. Training

1) Mandatory Training for All Contractor Staff. All Contractor (and/or any subcontractor) employees assigned to work on this contract shall complete the applicable HHS/OHS Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees shall complete HHS/OHS Information Security Awareness, Privacy, and Records Management training at least annually, during the life of this contract. All provided training shall be compliant with HHS training policies.

2) Role-based Training. All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the COR) must complete role-based training annually commensurate with their role and responsibilities in accordance with HHS policy and the HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum.

3) Training Records. The Contractor (and/or any subcontractor) shall maintain training records for all its employees working under this contract. A copy of the training records shall be provided to the CO and/or COR within 30 days after contract award and annually thereafter or upon request.

C. Rules of Behavior

1) The Contractor (and/or any subcontractor) shall ensure that all employees performing on the contract comply with the HHS Information Technology General Rules of Behavior.

2) All Contractor employees performing on the contract must read and adhere to the Rules of Behavior before accessing Department data or other information, systems, and/or networks that store/process government information, initially at the beginning of the contract and at least annually thereafter, which may be done as part of annual OHS Information Security Awareness Training. If the training is provided by the contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines.

D. Incident Response

FISMA defines an incident as “an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. The Contractor (and/or any subcontractor) shall comply with OHS’s Incident Response Policy dated July 10, 2018, including any subsequent updates.

In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) shall:

1) Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract so as to avoid a secondary sensitive information incident.

2) Notify affected individuals only as instructed by the Contracting Officer or designated representative.

3) Report all suspected and confirmed information security and privacy incidents and breaches to the OHS Incident Response Team (IRT), COR, CO, OHS SOP (or his or her designee), and other stakeholders, including incidents involving PII, in any medium or form, including paper, oral, or electronic as defined in OHS’s Incident Response Policy.

4) Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation.

E. Position Sensitivity Designations

All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR). The following position sensitivity designation levels apply to this solicitation/contract:

Non-Sensitive High Risk Tier 4 SF 85P

Roster. The Contractor (and/or any subcontractor) shall submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster shall be submitted to the COR and/or CO within 3 days of the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within 24 hours of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member. If the employee is filling a new position, the Contractor shall provide a position description and the Government will determine the appropriate suitability level.

F. Contract Initiation and Expiration

1) System Documentation. Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, Security Considerations in the System Development Life Cycle, at a minimum, for system development.

2) Sanitization of Government Files and Information. As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) shall provide all required documentation to the CO and/or COR to certify that, at the government’s direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, Guidelines for Media Sanitization.

3) Notification. The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO within 48 hours before an employee stops working under this contract.

4) Contractor Responsibilities Upon Physical Completion of the Contract. The contractor (and/or any subcontractors) shall return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor shall provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or OHS policies.

5) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the OHS Contractor Employee Separation Checklist when an employee terminates work under this contract within 3 days of the employee’s exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

G. Records Management and Retention

The Contractor (and/or any subcontractor) shall maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and HHS/OHS policies and shall not dispose of any records unless authorized by HHS/OHS.

In the event that a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, it shall be documented and reported as an incident in accordance with HHS/OHS policies.

## Records Management

A. Applicability

This clause applies to all Contractors whose employees create, work with, or otherwise handle Federal records, as defined in Section B, regardless of the medium in which the record exists.

B. Definitions

“Federal record” as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. The term Federal record:

* includes OHS records.
* does not include personal materials.
* applies to records created, received, or maintained by Contractors pursuant to their OHS contract.
* may include deliverables and documentation associated with deliverables.

C. Requirements

Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

Electronic information system means an information system that contains and provides access to computerized Federal records and other information. (36 CFR 1236.2)

The following types of records management controls are needed to ensure that Federal records in electronic information systems can provide adequate and proper documentation of agency business for as long as the information is needed. Agencies must incorporate controls into the electronic information system or integrate them into a recordkeeping system that is external to the information system itself. (36 CFR 1236.10)

1. Reliability: Controls to ensure a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.
2. Authenticity: Controls to protect against unauthorized addition, deletion, alteration, use, and concealment.
3. Integrity: Controls, such as audit trails, to ensure records are complete and unaltered.
4. Usability: Mechanisms to ensure records can be located, retrieved, presented, and interpreted.
5. Content: Mechanisms to preserve the information contained within the record itself that was produced by the creator of the record.
6. Context: Mechanisms to implement cross-references to related records that show the organizational, functional, and operational circumstances about the record, which will vary depending upon the business, legal, and regulatory requirements of the business activity.
7. Structure: Controls to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements.

In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

OHS and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of OHS or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report it to OHS immediately. The agency must report promptly to NARA in accordance with 36 CFR 1230.

The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the contract. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government’s behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to OHS control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the contract. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any subcontractor) is required to abide by Government and HHS and OHS guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with HHS and OHS policy.

The Contractor shall not create or maintain any records containing any non-public HHS or OHS information that are not specifically tied to or authorized by the contract.

The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

1. OHS owns the rights to all data and records produced as part of this contract. OHS shall have unlimited rights to use, dispose of, or disclose all data contained in any and all contract deliverables as it determines to be in the public interest and in accordance with the data rights clauses applicable to this contract

Training. All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take OHS-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

D. Flowdown of requirements to subcontractors

The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract, and require written subcontractor acknowledgment of same.

Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

## Contractor Transition

## Ensure and agree that all deliverables, products, licenses, designs, data, documentation, tests, user research notes, source code, configuration settings and files, and materials developed throughout this call order will be the property of the U.S. Government and in the public domain. One week prior to task order conclusion, all deliverables, products, will be incorporated into the project repository. Exclusion of project artifacts may be allowed in coordination with the OHS Product Owner and COR. Provide any other reasonable assistance to the Government to deploy the latest version application.

## 

## During the transition to the Government or a new contractor, the Contractor shall perform all necessary transition activities. Expected transition activities may include, but not be limited to:

## Continuation of full services to OHS and other customers

## Participation in meetings with the Government or a new contractor to effect a smooth transition and provide detailed information on the operation of all deliverables, at COR and the OHS Product Lead's discretion.

## Training of new personnel, either Government or a new contractor, during transition period Appropriate close-out of any outstanding technical and related performance elements for this task

## 

## Should the contractor be terminated prior to the end of the period of performance, the contractor shall transfer all project materials to the COR and the OHS Product Owner within two weeks of the COR and the OHS Product Owner’s request.

## 

1. **List of Security Deliverables**

|  |  |  |
| --- | --- | --- |
| Deliverable Name | Deliverable Title/Description | Due Date |
| Roster | Roster of all employees | Within 3 daysof the effective date of this contract |
| Contractor Employee Non-Disclosure Agreement (NDA) | Contractor Employee Non-Disclosure Agreement (NDA) | Prior to performing any work on behalf of HHS |
| Privacy Threshold Analysis (PTA)/ Privacy Impact Assessment (PIA) | Assist in the completion of a PTA/PIA form | Within 30 daysafter the contract award |
| Training Records | Copy of training records for all mandatory training | In conjunction with contract award and annually thereafter or upon request |
| Rules of Behavior | Signed ROB for all employees | Initiation of contract and at least annually thereafter |
| Incident Response Report | Incident Report (as incidents or breaches occur) | As soon as possible and without reasonable delay and no later than 1 hour of discovery |
| Incident Response Plan | Incident and Breach Response Plan | Upon request from government |
| Personnel Security Responsibilities (onboarding) | List of Personnel with defined roles and responsibilities | Within 3 daysthat is before an employee begins working on this contract. |
| Personnel Security Responsibilities (off-boarding) | Off-boarding documentation, equipment and badge when leaving contract | Within 3days after the Government’s final acceptance of the work under this contract, or in the event of a termination of the contract |
| Background Investigation Documentation | Onboarding documentation when beginning the contract | Prior to performing any work on behalf of HHS/OHS |
| Certification of Sanitization of Government and Government Activity-  Related Files, Information, and Devices | Form or deliverables required by OHS. | At contract expiration |
| Contract Initiation and Expiration | If the procurement involves a system or cloud service, additional documentation will be required, such as Disposition/Decommission Plan | At contract expiration |
| Security Assessment and Authorization (SA&A) | SA&A Package   * SSP * SAR * POA&M * Authorization Letter * CP and CPT Report * E-Auth (if applicable) * PTA/PIA (if applicable) * Interconnection/Data Use Agreements (if applicable) * Authorization Letter * Configuration Management Plan (if applicable) * Configuration Baseline * Other OHS-specific documents | Due date to be determined and approved by OHS OCIO based on planned deployment and ATO schedule |
| Reporting and Continuous Monitoring | Revised security documentation/Agreements | As required by OHS OCIO |
| Security Alerts, Advisories, and Directives | List of personnel with designated roles and responsibilities | As required by OHS OCIO |
| Incident Reporting | * Incident Reports (as needed) * Incident Response Plan | Incident Response plan provided in accordance with ATO schedule and yearly thereafter (Prior to production deployment or go live date)  Incident Reports provided quarterly and upon request |
| Other IT Procurements (Non-Commercial and Open Source Computer Software Procurements) | * Computer Software, including the source code | Prior to performing any work on behalf of HHS |

1. **Contract Provisions & Clauses**

All provisions and clauses included and accepted as part of the vendor’s GSA Schedule Contract flowdown to this RFQ.

**Contractor Team Arrangement (CTA)**

Contractor Team Arrangements (CTAs) are permitted. Note - FAR 9.6, Contractor Team Arrangements, does not apply to GSA Schedules teaming. Under GSA Schedules, Teaming allows contractors to use their individual GSA Schedules to develop a solution for the government.

{{*If the vendor intends to team, a CTA is required by the closing date and time of the RFQ. However, a fully executed CTA will be formalized at time of award. CTAs shall utilize and submit this* [*Attachment 1*](https://docs.google.com/document/d/1fUk_XbF8X_wseOMdpemXVKbAoNuasfooJatFcP0T7PA/edit) *- ID231XXXXXX - Contract Team Agreement when a CTA is applicable*.}}

CTAs will not be evaluated, but will be reviewed to:

* Gain an understanding of how the arrangement will work
* Identify any areas of responsibility that may require clarification
* Identify deficiencies in the CTA in order to understand the probability of successful performance
* Verify proposed prices/rates against MAS contract awarded prices/rates.

**Contract Provisions**

**52.252-1 Solicitation Provisions Incorporated by Reference (Feb 1998)**

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es): <https://www.acquisition.gov/browsefar>

**(End of provision)**

**GSAR 552.217-71 - Notice Regarding Option(s) (Nov 1992)**

The General Services Administration (GSA) has included an option to [Insert “purchase additional quantities of supplies or services” or “extend the term of this contract” or “purchase additional quantities of supplies or services and to extend the term of this contract”] in order to demonstrate the value it places on quality performance by providing a mechanism for continuing a contractual relationship with a successful Offeror that performs at a level which meets or exceeds GSA’s quality performance expectations as communicated to the Contractor, in writing, by the Contracting Officer or designated representative. When deciding whether to exercise the option, the Contracting Officer will consider the quality of the Contractor’s past performance under this contract in accordance with 48CFR517.207.

**(End of provision)**

**52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Dec 2019)**

**52.204-26 Covered Telecommunications Equipment or Services-Representation (Dec 2019)**

**Contract Clauses**

**FAR 52.252-2 -- Clauses Incorporated By Reference (Feb 1998)**

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): (<https://www.acquisition.gov/browsefar>)

**(End of clause)**

**FAR 52.203-18 Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements-Representation (Jan 2017)**

**FAR 52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)**

**FAR 52.212-4 Contract Terms and Conditions-Commercial Items (Oct 2018)**

**FAR 52.227-17 Rights in Data -- Special Works (DEC 2007)**

**GSAR 552.212-4 - Contract Terms and Conditions—Commercial Items (Feb 2018**)**(DEVIATION FAR 52.212-4)**

**GSAR 552.232-39 Unenforceability of Unauthorized Obligations. (FAR Deviation Feb 2018)**

**GSAR 552.238-82, Special Ordering Procedures for the Acquisition of Order-Level Materials**

**GSAR 552.204-70 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment.**

(a) Definitions. As used in this clause “covered telecommunications equipment or services", "Critical technology", and “substantial or essential component" have the meanings provided in FAR 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Prohibition. Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service 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. Contractors are not prohibited from providing-

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Representation. [Contractor to complete and submit to the Contracting Officer] The Offeror or Contractor represents that it [ ] will or [ ] will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract, order, or other contractual instrument resulting from this contract. This representation shall be provided as part of the proposal and resubmitted on an annual basis from the date of award.

(d) Disclosures. If the Offerer or Contractor has responded affirmatively to the representation In paragraph (c) of this clause, the Offeror or Contractor shall provide the following additional information to the Contracting Officer--

(1) All covered telecommunications equipment and services offered or provided (include brand; model number, such as original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(2) Explanation of the proposed use of covered telecommunications equipment and services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b) of this provision; 10

(3) For services, the entity providing the covered telecommunications services (include entity name, unique entity identifier, and Commercial and Government Entity (CAGE) code, if known); and

(4) For equipment, the entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known).

**(End of clause)**

#### 

**FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment**

As prescribed in [4.2105](https://acquisition.gov/content/part-4-administrative-matters#id1989H0G40RF)(b), insert the following clause:

Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2019)

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

“Covered foreign country” means The People’s Republic of China.

“Covered telecommunications equipment or services” means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) 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);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of 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.

“Critical technology” means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

“Substantial or essential component” means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.* Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service 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. The Contractor is prohibited from providing to the Government any equipment, system, or service 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, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in Federal Acquisition Regulation [4.2104](https://acquisition.gov/content/part-4-administrative-matters#id1989GI040ZO).

(c) *Exceptions.* This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement. (1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at [https://dibnet.dod.mil](https://dibnet.dod.mil/). For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at [https://dibnet.dod.mil](https://dibnet.dod.mil/).

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

**(End of clause)**

**FAR 52.217-8 - Option to Extend Services (Nov 1999)**

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 5 calendar days before the contract expires.

**(End of clause)**

**FAR 52.217-9 - Option to Extend the Term of the Contract (Mar 2000)**

(a) The Government may extend the term of this contract by written notice to the Contractor within 5 days provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 15 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 3 years.

**(End of clause)**