**SECTION K**

**REPRESENTATIONS, CERTIFICATIONS**

**AND OTHER STATEMENTS OF OFFERORS**

**Alternate A, System for Award Management.**

ALTERNATE I , SYSTEM FOR AWARD MANAGEMENT (OCT 2018)

      (a) Definitions. As used in this provision—

     “Electronic Funds Transfer (EFT) indicator means a four-character suffix to the unique entity identifier. The suffix is assigned at the discretion of the commercial, nonprofit, or Government entity to establish additional System for Award Management records for identifying alternative EFT accounts (see [subpart  32.11](https://www.acquisition.gov/content/subpart-3211-electronic-funds-transfer#i1080713)) for the same entity.

      Registered in the System for Award Management (SAM) means that–

           (1) The Offeror has entered all mandatory information, including the unique entity identifier and the EFT indicator, if applicable, the Commercial and Government Entity (CAGE) code, as well as data required by the Federal Funding Accountability and Transparency Act of 2006 (see [subpart  4.14](https://www.acquisition.gov/content/subpart-414-reporting-executive-compensation-and-first-tier-subcontract-awards#i1121746)) into SAM

           (2) The offeror has completed the Core, Assertions, and Representations and Certifications, and Points of Contact sections of the registration in SAM;

           (3) The Government has validated all mandatory data fields, to include validation of the Taxpayer Identification Number (TIN) with the Internal Revenue Service (IRS). The offeror will be required to provide consent for TIN validation to the Government as a part of the SAM registration process; and

           (4) The Government has marked the record “Active”.

      Unique entity identifier means a number or other identifier used to identify a specific commercial, nonprofit, or Government entity. See [www.sam.gov](http://www.sam.gov/) for the designated entity for establishing unique entity identifiers.

      (b)(1) An Offeror is required to be registered in SAM as soon as possible. If registration is not possible when submitting an offer or quotation, the awardee shall be registered in SAM in accordance with the requirements of clause [52.204-13](https://www.acquisition.gov/content/52204-13-system-award-management-maintenance#i1064160), System for Award Management Maintenance.

           (2) The Offeror shall enter, in the block with its name and address on the cover page of its offer, the annotation “Unique Entity Identifier” followed by the unique entity identifier that identifies the Offeror's name and address exactly as stated in the offer. The Offeror also shall enter its EFT indicator, if applicable. The unique entity identifier will be used by the Contracting Officer to verify that the Offeror is registered in the SAM.

      (c) If the Offeror does not have a unique entity identifier, it should contact the entity designated at [www.sam.gov](http://www.sam.gov/) for establishment of the unique entity identifier directly to obtain one. The Offeror should be prepared to provide the following information:

           (1) Company legal business name.

           (2) Tradestyle, doing business, or other name by which your entity is commonly recognized.

           (3) Company physical street address, city, state, and Zip Code.t

           (4) Company mailing address, city, state and Zip Code (if separate from physical).

           (5) Company telephone number.

           (6) Date the company was started.

           (7) Number of employees at your location.

           (8) Chief executive officer/key manager.

           (9) Line of business (industry).

           (10) Company headquarters name and address (reporting relationship within your entity).

      (d) Processing t ime should be taken into consideration when registering. Offerors who are not registered in SAM should consider applying for registration immediately upon receipt of this solicitation. See [https://ww.sam.gov](http://www.sam.gov/) for information on registration.

(End of provision)

**Identification and Assertion of Use, Release, or Disclosure Restrictions.**

I**DENTIFICATION AND ASSERTION OF USE, RELEASE, OR DISCLOSURE RESTRICTIONS**

(a) The terms used in this provision are defined in following clause or clauses contained in this solicitation—

(1) If a successful offeror will be required to deliver technical data, the Rights in Technical Data--Noncommercial Items clause, or, if this solicitation contemplates a contract under the Small Business Innovation Research Program, the Rights in Noncommercial Technical Data and Computer Software--Small Business Innovation Research (SBIR) Program clause.

(2) If a successful offeror will not be required to deliver technical data, the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation clause, or, if this solicitation contemplates a contract under the Small Business Innovation Research Program, the Rights in Noncommercial Technical Data and Computer Software--Small Business Innovation Research (SBIR) Program clause.

(b) The identification and assertion requirements in this provision apply only to technical data, including computer software documentation, or computer software to be delivered with other than unlimited rights. For contracts to be awarded under the

Small Business Innovation Research Program, the notification and identification requirements do not apply to technical data or computer software that will be generated under the resulting contract. Notification and identification is not required for restrictions based solely on copyright.

(c) Offers submitted in response to this solicitation shall identify, to the extent known at the time an offer is submitted to the Government, the technical data or computer software that the Offeror, its subcontractors or suppliers, or potential subcontractors or suppliers, assert should be furnished to the Government with restrictions on use, release, or disclosure.

(d) The Offeror's assertions, including the assertions of its subcontractors or suppliers or potential subcontractors or suppliers, shall be submitted as an attachment to its offer in the following format, dated and signed by an official authorized to contractually obligate the Offeror:

Identification and Assertion of Restrictions on the Government's Use, Release, or Disclosure of Technical Data or Computer Software.

The Offeror asserts for itself, or the persons identified below, that the Government's rights to use, release, or disclose the following technical data or computer software should be restricted:

|  |  |  |  |
| --- | --- | --- | --- |
| Technical Data or |  |  |  |
| Computer Software |  |  | Name of Person |
| to be Furnished | Basis for | Asserted Rights | Asserting |
| With Restrictions\* | Assertion\*\* | Category\*\*\* | Restrictions\*\*\*\* |
| (LIST)\*\*\*\*\* | (LIST) | (LIST) | (LIST) |

\*For technical data (other than computer software documentation) pertaining to items, components, or processes developed at private expense, identify both the deliverable technical data and each such item, component, or process. For computer software or computer software documentation identify the software or documentation.

\*\*Generally, development at private expense, either exclusively or partially, is the only basis for asserting restrictions. For technical data, other than computer software documentation, development refers to development of the item, component, or process to which the data pertain. The Government's rights in computer software documentation generally may not be restricted. For computer software, development refers to the software. Indicate whether development was accomplished exclusively or partially at private expense. If development was not accomplished at private expense, or for computer software documentation, enter the specific basis for asserting restrictions.

\*\*\*Enter asserted rights category (e.g., government purpose license rights from a prior contract, rights in SBIR data generated under another contract, limited, restricted, or government purpose rights under this or a prior contract, or specially negotiated licenses).

\*\*\*\*Corporation, individual, or other person, as appropriate.

\*\*\*\*\*Enter “none” when all data or software will be submitted without restrictions.

|  |  |
| --- | --- |
| Date | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Printed Name and Title | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Signature | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

(End of identification and assertion)

(e) An offeror's failure to submit, complete, or sign the notification and identification required by paragraph (d) of this provision with its offer may render the offer ineligible for award.

(f) If the Offeror is awarded a contract, the assertions identified in paragraph (d) of this provision shall be listed in an attachment to that contract. Upon request by the Contracting Officer, the Offeror shall provide sufficient information to enable the Contracting Officer to evaluate any listed assertion.

(End of provision)

**TECHNICAL DATA OR COMPUTER SOFTWARE PREVIOUSLY DELIVERED TO THE GOVERNMENT**

The Offeror shall attach to its offer an identification of all documents or other media incorporating technical data or computer software it intends to deliver under this contract with other than unlimited rights that are identical or substantially similar to documents or other media that the Offeror has produced for, delivered to, or is obligated to deliver to the Government under any contract or subcontract. The attachment shall identify—

(a) The contract number under which the data or software were produced;

(b) The contract number under which, and the name and address of the organization to whom, the data or software were most recently delivered or will be delivered; and

(c) Any limitations on the Government's rights to use or disclose the data or software, including, when applicable, identification of the earliest date the limitations expire.

investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

**COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS**

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

“Controlled technical information,” “covered contractor information system,” “covered defense information,” “cyber incident,” “information system,” and “technical information” are defined in Defense Federal Acquisition Regulations Supplement (DFARS) clause [252.204-7012](http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012), Safeguarding Covered Defense Information and Cyber Incident Reporting or Article XII of the attached OTA.

(b) The security requirements required by contract clause DFARS [252.204-7012](http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012) or Article XII of the attached OTA, shall be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract.

(c) For covered contractor information systems that are not part of an information technology service or system operated on behalf of the Government (see DFARS [252.204-7012](http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012)(b)(2) or Article XII of the attached OTA —

(1) By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” (see <http://dx.doi.org/10.6028/NIST.SP.800-171>) that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017.

(2) (i) If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 that are in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of—

(A) Why a particular security requirement is not applicable; or

(B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.

(ii) An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.

(End of provision)

**SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016)**

(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.

“Contractor 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 contractor(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 contractor 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 Government-wide 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](http://www.acq.osd.mil/dpap/dars/dfars/html/current/252227.htm#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 Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor 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 DFARS clause [252.239-7010](http://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm#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 Contractor 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 Contractor shall notify the DoD Chief Information Officer (CIO), via email at [osd.dibcsia@mail.mil](mailto:osd.dibcsia@mail.mil), within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract 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 Contractor 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 Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (<https://www.fedramp.gov/resources/documents/>) 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 Contractor 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 Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor’s ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

(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 Contractor’s network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor’s ability to provide operationally critical support; and

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

(3) *Medium assurance certificate requirement*. In order to report cyber incidents in accordance with this clause, the Contractor 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 <http://iase.disa.mil/pki/eca/Pages/index.aspx>.

(d) *Malicious software*. When the Contractor 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 Contractor discovers a cyber incident has occurred, the Contractor 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 Contractor 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 Contractor 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 contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor 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 contractor 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 contractor (“recipient”) that is directly supporting Government activities under a contract that includes the DFARS clause at [252.204-7009](http://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7009), Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) *Use and release of contractor attributional/proprietary information 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 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 Contractor 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 Contractor’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 Contractor shall—

(1) Include this clause, 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 Contractor 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 prime Contractor (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 prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

(End of clause)

**REPRESENTATION OF USE OF CLOUD COMPUTING (SEP 2015**)

(a) *Definition*. “Cloud computing,” as used in this provision, means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

(b) The Offeror shall indicate by checking the appropriate blank in paragraph (c) of this provision whether the use of cloud computing is anticipated under the resultant contract.

(c) *Representation*. The Offeror represents that it—

\_\_\_\_\_ Does anticipate that cloud computing services will be used in the performance of any contract or subcontract resulting from this solicitation.

\_\_\_\_\_ Does not anticipate that cloud computing services will be used in the performance of any contract or subcontract resulting from this solicitation.

**Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2020)**

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it “does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument” in the following provision, Covered Telecommunications Equipment or Services—Representation.

      (a) Definitions. As used in this provision—

      Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in Article XV of attached OTA template, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

      (b) Prohibition.

(1) 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. Nothing in the prohibition shall be construed to—

                (i)Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

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

           (2) Section 889(a)(1)(B) 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, 2020, from entering into a contract or extending or renewing a contract with an entity that uses 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. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

                (i)Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

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

      (c) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) ([https://www.sam.gov](https://www.sam.gov/)) for entities excluded from receiving federal awards for “covered telecommunications equipment or services”.

      (d) Representation. The Offeror represents that—

           (1)It □ will, □ will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds “will” in paragraph (d)(1) of this section; and

           (2)After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that—

          It □ does, □ does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds “does” in paragraph (d)(2) of this section.

      (e) Disclosures.

(1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded “will” in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:

                (i)For covered equipment—

                     (A)The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

                     (B)A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

                     (C)Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

                (ii)For covered services—

                     (A)If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

                     (B)If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

           (2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded “does” in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

                (i)For covered equipment—

                     (A)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);

                     (B)A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

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

                (ii)For covered services—

                     (A)If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

                     (B)If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision

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

      (a) Definitions. As used in this provision, “covered telecommunications equipment or services” has the meaning provided in the article, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

      (b) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) ([https://www.sam.gov](https://www.sam.gov/)) for entities excluded from receiving federal awards for “covered telecommunications equipment or services”.

      (c) Representation. The Offeror represents that it □ does, □ does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(end of provision)

**252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements.**

As prescribed in 204.7304(d), use the following provision:

NOTICE OF NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)

(a) *Definitions*.

“Basic Assessment”, “Medium Assessment”, and “High Assessment” have the meaning given in the clause 252.204-7020, NIST SP 800-171 DoD Assessments.

“Covered contractor information system” has the meaning given in ARTICLE XI Operational Security and ARTICLE XII Cyber Security and Incident Reporting, of the attached OTA.

(b) *Requirement*. In order to be considered for award, if the Offeror is required to implement NIST SP 800-171, the Offeror shall have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see ARTICLE XIV) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800-171 DoD Assessments are described in the NIST SP 800-171 DoD Assessment Methodology located at <https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html>.

(c) *Procedures*.

(1) The Offeror shall verify that summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) (<https://www.sprs.csd.disa.mil/>) for all covered contractor information systems relevant to the offer.

(2) If the Offeror does not have summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the Offeror may conduct and submit a Basic Assessment to <mailto:webptsmh@navy.mil> for posting to SPRS in the format identified in paragraph (d) of this provision.

(d) *Summary level scores*. Summary level scores for all assessments will be posted 30 days post-assessment in SPRS to provide DoD Components visibility into the summary level scores of strategic assessments.

(1) *Basic Assessments*. An Offeror may follow the procedures in paragraph (c)(2) of this provision for posting Basic Assessments to SPRS.

(i) The email shall include the following information:

(A) Cybersecurity standard assessed (e.g., NIST SP 800-171 Rev 1).

(B) Organization conducting the assessment (e.g., Contractor 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 (d)(1)(i) of this section, the Offeror 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 achieved |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

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

(3) *Accessibility*.

(i) 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).

(ii) Authorized representatives of the Offeror 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>.

(iii) A High NIST SP 800-171 DoD Assessment may result in documentation in addition to that listed in this section. 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 contractor that is privileged or confidential).

(End of provision)

**Foreign Persons (2006) Section K**   
   
In accordance with restrictions required by Executive Order 12470, the Arms Export Control Act (Title 22, USC) (Sec 275), the International Traffic in Arms Regulation (ITAR), or DoD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure, no foreign persons will be permitted to work on a contract without notifying the Contracting Officer. Provide the following information for all foreign persons who will be working on the contract (or “X” here if there are no such individuals: \_\_\_\_):

(1) Full Name:   
(2) Date of Birth:   
(3) Place of Birth:   
(4) Nationality:   
(5) Social Security Number:   
(6) Visa Status:   
(7) Current Address:   
(8) If a Subcontractor, Subcontractor Name and Address:   
(9) Biographic data and/or resume:

**Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law (Feb 2016)**

(a) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L 113-235), and similar provisions, if contained in subsequent appropriations acts, the Government will not enter into a contract with any corporation that--

(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(b) The Offeror represents that—

(1) It is [ ] is not [ ] a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(2) It is [ ] is not [ ] a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

This is to certify that, as an authorized representative of the company, the information provided in the above responses is true and correct to the best of my knowledge and belief:

|  |  |
| --- | --- |
| Date | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Printed Name and Title | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Signature | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |