PART II - CONTRACT CLAUSES

SECTION I
CONTRACT CLAUSES

52.232 18
PAYMENT REQUESTS AND RECEIVING REPORTS DEC 2018

52.219 28
PST AWARD SMALL BUSINESS PR GRAM REPRESENTATI N JUL 2019

(T) Definitions. As used in this clause-
"Long-TeTm conTTTct" meTns T conTTTct of moTe ThTn five yeTTs in duTTTion, including OTTions. However, The TeTm does not include conTTTcTs ThT exceed five yeTTs in duTTTion becTuse The TeTioT of TeTfoTMmcTe its been exTeended foT T cumuTTive TeTioT not to exceed six monThs unDeT the clTuse TT 6T.TT-8, OTTion To Extende TTervices, or oT heT
TTTTOTTITTTe TuTToty.

"SmTll business conceTn" meTns T conceTn, including its TffilTTTes, ThT is in deTeNeNdly owneTe TnT oTTeTTTed, NOT domiTnTn in the field of oTTeTTTion in which it is bidding on GoveTeMenTT conTTTcTs, TnT quTTified Ts T smTll business und eT the cTTTeTIT1 in 13 CFR TTTT T11 Tnd The size sTTnTdTdT in TTTTgTTTth (c) of T his clTuse. Such T conceTn is "NOT domiTnTn in its field of oTTeTTTion" when it does not exTeCTe T conTTolling oT TTTjT influence on T nTTionT1 bTts in T kind of business TcTTiviTy in which T number of business conceTns TTe TTTimTTITly enTTTed. In deTeTTining wheTheT domiTnTn exists, conTTTTion sTTll be given To T11 TTTTOTTITTTe FTCToTs, including volume of business, number of emTTloyees, ffinTTcTTTes, tegTTcTTTes, comTTTTive sTTITus oT TOSITion, owneTTshIT oT conTTol of mTTTeTTITs, TToTTesses, TTTenTs, license TgTeemenTs, FTCiTTies, sTTes TTTIToT, TnT nTTuTe of business TcTTiviTy.

If The ConTTTcTOTr TeTTeTsenTed ThTT is wTs T smTll business conceTn TTIOTr To TwTTd of TTTTTCT, The ConTTTcTOTr sTTll TeTeTTeTsenT its size stTTUs TccOTITing To TTTTTTTTT (e) of TTTTTTTTTc, if TTTTTITleTle, TTTTTTTTT (g) of TTTTTTTTTc, uTnT the occuTTTTTion of Tncy of The following:

(I) WitTTn 30 dTTs TTTTeT execution of T novTTIOTr TgTeemenT oT witTTn 30 dTTs TTTTeT modificTTion of The ConTTTTCT to include this clTTuse, if the novTTIOTr TgTeemenT wTs exeCuTTTed TTIOTr to incTusion of this clTTuse in the ConTTTTCT.

(T) WitTTn 30 dTTs TTTTeT T meTTget oT TquTTsITion ThTT does not TeqUITe T novTTIOTr oT witTTn 30 dTTs TTTTeT modificTTion of The conTTTTCT to include this clTTuse, if The meTTget oT TquTTsITion occuTTTTd TTIOTr to incTusion of this clTTuse in the ConTTTTCT.

(3) For long-term contracts-

(i) WitTTn 60 to 120 days prior to the end of the fifth year of the contract; and
(ii) WitTTn 60 to 120 days prior to the date specified in the contract for exercising any option thereafter.

(c) The Contractor shall rerepresent its size status in accordance with the size standard in effect at the time of this rerepresentation that corresponds to the North American Industry Classification System (NAICS) code assigned to this contract. The small business size standard corresponding to this NAICS code can be found at: http://www.sba.gov/content/table-small-business-size-standards.
252.219-28 POST-AWARD SMALL BUSINESS PROGRAM REPRESENATATION (JUL 2013)

(d) The small business size standard for a Contractor providing a product which it does not manufacture itself, for a contract other than a construction or service contract, is 500 employees.

(e) Except as provided in paragraph (g) of this clause, the Contractor shall make the representation required by paragraph (b) of this clause by validating or updating all its representations in the Representations and Certifications section of the System for Award Management (SAM) and its other data in SAM, as necessary, to ensure that they reflect the Contractor's current status. The Contractor shall notify the contracting office in writing within the timeframe specified in paragraph (b) of this clause, that the data have been validated or updated, and provide the date of the validation or update.

(f) If the Contractor represented that it was other than a small business concern prior to award of this contract, the Contractor may, but is not required to, take the actions required by paragraphs (e) or (g) of this clause.

(g) If the Contractor does not have representations and certifications in SAM, or does not have a representation in SAM for the NAICS code applicable to this contract, the Contractor is required to complete the following rerepresentation and submit it to the contracting office, along with the contract number and the date on which the rerepresentation was completed:

The Contractor represents that it ( ) is, ( ) is not a small business concern under NAICS Code __________________ assigned to contract number _____________________. (Contractor to sign and date and insert authorized signers' name and title)

252.204-7012 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 n or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—
252.204-7012 (CDT)
SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT
REPORTING (OCT 2018)

(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 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 an information system.

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

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

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) Adequate security. The 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 clause 252.239-7010, Cloud Computing Services, of this contract.

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

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:
(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(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, the Contractor shall—

(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.

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

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

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

(ii) (A) The 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, 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 system security measures when the Contractor reasonably determines that
252.204-7012 (CDT)
SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT
REPORTING (OCT 2016)

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 contractors ability to perform the requirements off 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 Contractors 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 Contractors 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://iae.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 clause at 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) Requires 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.

252.204-7015
NOTICE OF AUTHORIZED DISCLOSURE OF INFORMATION FOR LITIGATION SUPPORT (MAY 2016)
e Use or Disclosure of Information by Litigation Support Contractors.
NOTICE OF AUTHORIZED DISCLOSURE OF INFORMATION FOR LITIGATION SUPPORT (MAY 2016)

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

"Litigation support" means administrative, technical, or professional services provided in support of the Government during or in anticipation of litigation.

"Litigation support contractor" means a contractor (including its experts, technical consultants, subcontractors, and suppliers) providing litigation support under a contract that contains the clause at 252.204-7014, itation or contract, the Government may disclose to a litigation support contractor, for the sole purpose of litigation support activities, any information, including sensitive information, received—

"Sensitive information" means controlled unclassified information of a commercial, financial, proprietary, or privileged nature. The term includes technical data and computer software, but does not include information that is lawfully, publicly available without restriction.

"Technical data" means recorded information, regardless of the form or method of the recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial and/or management information.

(b) Notice of authorized disclosures. Notwithstanding any other provision of this solicitation or contract, the Government may disclose to a litigation support contractor, for the sole purpose of litigation support activities, any information, including sensitive information, received—

(1) Within or in connection with a quotation or offer; or
(2) In the performance of or in connection with a contract.

(c) Flowdown. Include the substance of this clause, including this paragraph (c), in all subcontracts, including subcontracts for commercial items.

52.204-7014

52.202-20

52.209-10

52.203-19

52.204-7014 (CONT)

52.202-20

52.209-10

52.203-19

52.204-7014 (CONT)

52.202-20

52.209-10

52.203-19

52.204-7014 (CONT)

52.202-20

52.209-10

52.203-19

52.204-7014 (CONT)

52.202-20