FEDERAL ACQUISITION REGULATION (FAR) AND DEFENSE FAR SUPPLEMENT (DFARS) FLOWDOWN PROVISIONS
CONTRACT HQ0147-18-C-0023

The FAR and DFARS clauses cited below are incorporated herein by reference as the effective version found in PeopleTec's Prime Contract. The listed FAR and DFARS clauses are incorporated herein as if set forth in full text unless made inapplicable by its corresponding note, if any. "Contractor" means "Consultant," "Contracting Officer" means "PeopleTec," "Contract" means this Agreement and "Government" means "PeopleTec or the Government." However, the words "Government" and "Contracting Officer" do not change: (1) when a right, act, authorization or obligation can be granted or performed only by the Government or the Government Contracting Officer or duly authorized representative, and (2) when title to property is to be transferred directly to the Government.

Clause	FAR Reference
Gratuities	52.203-3
Security Requirements	52.204-2
NOTE: Delete paragraph (c). NOTE: Applicable if this Order involves access to Classified Information.	
Personal Identity Verification of Contractor Personnel	52.204-9
Certification for Federal Funding Accountability and Transparency Act (FFATA)	52.204-10
Basic Safeguarding of Covered Contractor Information Systems	52.204-21
Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended or Proposed for Debarment	52.209-6
Defense Priority and Allocation Requirements	52.211-15
This is a rated order DX-C9 certified for national defense, emergency preparedness, and energy program use, and the Contractor shall follow all the requirements of the Defense Priorities and Allocations System regulation (15 CFR 700).	
Utilization of Small Business Concerns	52.219-8
Prohibition of Segregated Facilities	52.222-21
Equal Opportunity	52.222-26
Affirmative Action for Workers with Disabilities	52.222-36
Notification of Employee Rights Under the National Labor Relations Act	52.222-40
Employment Eligibility Verification	52.222-54
Encouraging Contractor Policies to Ban Text Messaging While Driving	52.223-18
Restrictions on Certain Foreign Purchases	52.225-13
Preference for U.S. Flag Carriers	52.247-63
Prohibition on Persons Convicted of Fraud or Other Defense Contract-Related Felonies	252.203-7001
Requirement to Inform Employees of Whistleblower Rights	252.203-7002
Restrictions on the Use of Mandatory Arbitration Agreements	252.222-7006
Ground and Flight Risk	252.228-7001

GUARDING 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 Governmentwide policies, and is--

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

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

Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Forensic analysis means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Malicious software means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an

information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

Media means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

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

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

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

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

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

(3)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:

- 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 aspractical, 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.

(c) 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.

(d) 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.

(e) 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.

(1) 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.

(2) 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.

(3) 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.

(4) 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.

(5) 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.

(6) 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--

- To entities with missions that may be affected by such information;
- To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;
- To Government entities that conduct counterintelligence or law enforcement investigations;
- 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
- To a support services contractor (``recipient'') that is directly supporting Government activities under a contract e clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(4) 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.

(5) 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.

(6) 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.

(7) Subcontracts. The Contractor shall--

- 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

- Require subcontractors to--

    - 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

    - 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.

252.222-7000 RESTRICTIONS ON EMPLOYMENT OF PERSONNEL (MAR 2000)

(1) The Contractor shall employ, for the purpose of performing that portion of the contract work in the U.S, individuals who are residents thereof and who, in the case of any craft or trade, possess or would be able to acquire promptly the necessary skills to perform the contract.

(2) The Contractor's paragraph (b), in each subcontract awarded under this contract.

52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any Defense Federal Acquisition Regulation Supplement (DFARS) (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

252.203-7999 PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS (DEVIATION 2015-O0010) (FEB 2015)

(a) The Contractor shall not require employees or subcontractors seeking to report fraud, waste, or abuse to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or contactors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(b) The Contractor shall notify employees that the prohibitions and restrictions of any internal confidentiality agreements covered by this clause are no longer in effect.

(c) The prohibition in paragraph (a) of this clause does not contravene requirements applicable to Standard Form 312, Form 4414, or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(d)(1) In accordance with section 743 of Division E, Title VIII, of the Consolidated and Further Continuing Resolution Appropriations Act, 2015, (Pub. L. 113-235), use of funds appropriated (or otherwise made available) under that or any other Act may be prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this clause.
(2) The Government may seek any available remedies in the event the Contractor fails to perform in accordance with the terms and conditions of the contract as a result of Government action under this clause.

(End of clause)