

**FEDERAL ACQUISITION REGULATION (FAR) AND DEFENSE FAR  
SUPPLEMENT (DFARS) FLOWDOWN PROVISIONS  
PRIME CONTRACT W91260-20-F-D504  
SAIC SUBCONTRACT P010256802  
SAIC SUBCONTRACT 1116**

The FAR and DFARS clauses cited below are flowed down from the Prime Contract and Subcontract named above. The listed FAR and DFARS clauses are incorporated in purchase orders and subcontracts issued by PeopleTec and referencing the prime or subcontract number as if set forth in full text unless made inapplicable by its corresponding note, if any. “Contractor” means “Subcontractor,” “Supplier,” “Seller,” “Vendor,” or “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.

<b>FAR Reference</b>	<b>Clause</b>	<b>Effective Date</b>
52.203-3	Gratuities	APR 1984
52.203-6	Restrictions on Subcontractor Sales to the Government	SEP 2006
52.203-7	Anti-Kickback Procedures	MAY 2014
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	MAY 2014
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	MAY 2014
52.203-11	Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions	SEP 2007
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	OCT 2010
52.203-13	Contractor Code of Business Ethics and Conduct	OCT 2015
52.203-17	Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights	APR 2014
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements	JAN 2017
52.204-2	Security Requirements	AUG 1996
	NOTE: Delete paragraph (c). NOTE: Applicable if this Order involves access to Classified Information.	
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	JUL 2013
52.204-21	Basic Safeguarding of Covered Contractor Information System (if Seller may have Federal contract information, as defined in the clause, residing in or transiting through its information system)	NOV 2021
52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities	NOV 2021
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment	NOV 2021
52.209-6	Protecting the Government’s Interest When Subcontracting with Contractors Debarred, Suspended or Proposed for Debarment	AUG 2013
52.211-15	Defense Priority and Allocation Requirements 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).	APR 2008

52.219-8	Utilization of Small Business Concerns	NOV 2016
52.222-3	Convict Labor	JUN 2003
52.222-21	Prohibition of Segregated Facilities	FEB 1999
52.222-26	Equal Opportunity	SEP 2016
52.222-20	Contracts for Materials, Supplies, Articles, and Equipment Exceeding \$15,000 (if Subcontract is for manufacture or furnishing of materials, supplies, articles or equipment)	JUN 2020
52.222-35	Equal Opportunity for Veterans	OCT 2015
52.222-36	Equal Opportunity for Workers with Disabilities	OCT 2015
52.222-37	Employment Reports on Veterans	FEB 2016
52.222-40	Notification of Employee Rights Under the National Labor Relations Act	DEC 2010
562.222-50	Combatting Trafficking in Persons	FEB 2021
52.222-54	Employment Eligibility Verification	OCT 2015
52.223-6	Drug-Free Workplace	MAY 2001
52.223-18	Encouraging Contractor Policies to Ban Text Messaging While Driving	AUG 2011
52.225-13	Restrictions on Certain Foreign Purchases	JUN 2008
52.246-4	Inspection of Services – Fixed-Price	AUG 1996
52.247-64	Preference for Privately Owned U.S. Flag Commercial Vessels	NOV 2021
252.203-7001	Prohibition on Persons Convicted of Fraud or Other Defense Contract-Related Felonies	DEC 2008
252.203-7002	Requirement to Inform Employees of Whistleblower Rights	SEP 2013
252.204-7000	Disclosure of Information	OCT 2016
252.204-7004	Antiterrorism Awareness Training for Contractors (if Subcontract performance requires routine physical access to Federally-controlled facility or military installation)	FEB 2019
252.204-7015	Notice of Authorized Disclosure of Information for Litigation Support	MAY 2016
252.204-7018	Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services	DEC 2019
252.209-7004	Subcontracting with Firms That Are Owned or Controlled by the Government of a Terrorist Country	MAY 2019
252.223-7008	Prohibition of Hexavalent Chromium	JUN 2013
252.222-7006	Restrictions on the Use of Mandatory Arbitration Agreements	DEC 2010
252.225-7012	Preference for Certain Domestic Commodities	DEC 2017
252.225-7048	Export-Controlled Items	JUN 2013
252.247-7023	Transportation of Supplies by Sea	APR 2014
252.247-7024	Notification Of Transportation of Supplies by Sea	MAR 2000

52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)

(a) Definitions. As used in this clause--

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (*i.e.*, information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) *Other requirements.* This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial products or commercial services, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of clause)

## 252.204-7009 LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION

(a) Definitions. As used in this clause—

“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.

“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 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.

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

“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.

“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) Restrictions. The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party’s reporting of a cyber incident pursuant to DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause):

(1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 252.204-7012 and shall not be used for any other purpose.

(2) The Contractor shall protect the information against unauthorized release or disclosure.

(3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.

(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause.

(5) A breach of these obligations or restrictions may subject the Contractor to—

(i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and

(ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause.

(c) Subcontracts. The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.

(End of clause)

#### 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 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) 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.

(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 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.

(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.

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 contractors 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)

52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)

(a) Definitions. As used in this clause--

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means--

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

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

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

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

Critical technology means--

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

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

controlled--

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

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

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

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

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

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

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

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

(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. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Reserved.

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

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

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

(d) Reporting requirement.

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

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

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

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

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

252.211-7003 ITEM UNIQUE IDENTIFICATION AND VALUATION (DEC 2013)

(a) Definitions. As used in this clause Automatic identification device means a device, such as a reader or interrogator, used to retrieve data encoded on machine-readable media.

Concatenated unique item identifier means—(1) For items that are serialized within the enterprise identifier, the linking together of the unique identifier data elements in order of the issuing agency code, enterprise identifier, and unique serial number within the enterprise identifier; or (2) For items that are serialized within the original part, lot, or batch number, the linking together of the unique identifier data elements in order of the issuing agency code; enterprise identifier; original part, lot, or batch number; and serial number within the original part, lot, or batch number.

Data Matrix means a two-dimensional matrix symbology, which is made up of square or, in some cases, round modules arranged within a perimeter finder pattern and uses the Error Checking and Correction 200 (ECC200) specification found within International Standards Organization (ISO)/International Electrotechnical Commission (IEC) 16022. Data qualifier means a specified character (or string of characters) that immediately precedes a data field that defines the general category or intended use of the data that follows. DoD recognized unique identification equivalent means a unique identification method that is in commercial use and has been recognized by DoD. All DoD recognized unique identification equivalents are listed at [http://www.acq.osd.mil/dpap/pdi/uid/iuid\\_equivalents.html](http://www.acq.osd.mil/dpap/pdi/uid/iuid_equivalents.html).

DoD item unique identification means a system of marking items delivered to DoD with unique item identifiers that have machine-readable data elements to distinguish an item from all other like and unlike items. For items that are serialized within the enterprise identifier, the unique item identifier shall include the data elements of the enterprise identifier and a unique serial number. For items that are serialized within the part, lot, or batch number within the enterprise identifier, the unique item identifier shall include the data elements of the enterprise identifier; the original part, lot, or batch number; and the serial number.

Enterprise means the entity (e.g., a manufacturer or vendor) responsible for assigning unique item identifiers to items.

Enterprise identifier means a code that is uniquely assigned to an enterprise by an issuing agency. Government's unit acquisition cost means—(1) For fixed-price type line, subline, or exhibit line items, the unit price identified in the contract at the time of delivery; (2) For cost-type or undefinitized line, subline, or exhibit line items, the Contractor's estimated fully burdened unit cost to the Government at the time of delivery; and (3) For items produced under a time-and-materials contract, the Contractor's estimated fully burdened unit cost to the Government at the time of delivery.

Issuing agency means an organization responsible for assigning a globally unique identifier to an enterprise (e.g., Dun & Bradstreet's Data Universal Numbering System (DUNS) Number, GS1 Company Prefix, Allied Committee 135 NATO Commercial and Government Entity (NCAGE)/Commercial and Government Entity (CAGE) Code, or the Coded Representation of the North American Telecommunications Industry Manufacturers, Suppliers, and Related Service Companies (ATIS-0322000) Number), European Health Industry Business Communication Council (EHIBCC) and Health Industry Business Communication Council (HIBCC)), as indicated in the Register of Issuing Agency Codes for ISO/IEC 15459, located at <http://www.nen.nl/web/Normen-ontwikkelen/ISOIEC-15459-Issuing-Agency-Codes.htm>.

Issuing agency code means a code that designates the registration (or controlling) authority for the enterprise identifier.

Item means a single hardware article or a single unit formed by a grouping of subassemblies, components, or constituent parts.

Lot or batch number means an identifying number assigned by the enterprise to a designated group of items, usually referred to as either a lot or a batch, all of which were manufactured under identical conditions.

Machine-readable means an automatic identification technology media, such as bar codes, contact memory buttons, radio frequency identification, or optical memory cards.

Original part number means a combination of numbers or letters assigned by the enterprise at item creation to a class of items with the same form, fit, function, and interface.

Parent item means the item assembly, intermediate component, or subassembly that has an embedded item with a unique item identifier or DoD recognized unique identification equivalent.

Serial number within the enterprise identifier means a combination of numbers, letters, or symbols assigned by the enterprise to an item that provides for the differentiation of that item from any other like and unlike item and is never used again within the enterprise.

Serial number within the part, lot, or batch number means a combination of numbers or letters assigned by the enterprise to an item that provides for the differentiation of that item from any other like item within a part, lot, or batch number assignment.

Serialization within the enterprise identifier means each item produced is assigned a serial number that is unique among all the tangible items produced by the enterprise and is never used again. The enterprise is responsible for ensuring unique serialization within the enterprise identifier.

Serialization within the part, lot, or batch number means each item of a particular part, lot, or batch number is assigned a unique serial number within that part, lot, or batch number assignment. The enterprise is responsible for ensuring unique serialization within the part, lot, or batch number within the enterprise identifier.

Type designation means a combination of letters and numerals assigned by the Government to a major end item, assembly or subassembly, as appropriate, to provide a convenient means of differentiating between items having the same basic name and to indicate modifications and changes thereto.

Unique item identifier means a set of data elements marked on items that is globally unique and unambiguous. The term includes a concatenated unique item identifier or a DoD recognized unique identification equivalent.

Unique item identifier type means a designator to indicate which method of uniquely identifying a part has been used. The current list of accepted unique item identifier types is maintained at [http://www.acq.osd.mil/dpap/pdi/uid/uid\\_types.html](http://www.acq.osd.mil/dpap/pdi/uid/uid_types.html).

(b) The Contractor shall deliver all items under a contract line, subline, or exhibit line item.

(c) Unique item identifier. (1) The Contractor shall provide a unique item identifier for the following:

(i) Delivered items for which the Government's unit acquisition cost is \$5,000 or more, except for the following line items:

-----  
Contract line, subline, or exhibit line item No. Item description  
-----

-----

(ii) Items for which the Government's unit acquisition cost is less than \$5,000 that are identified in the Schedule or the following table:

-----  
Contract line, subline, or exhibit line item No. Item description  
-----

-----  
(If items are identified in the Schedule, insert "See Schedule" in this table.)

(iii) Subassemblies, components, and parts embedded within delivered items, items with warranty requirements,

DoD serially managed reparable and DoD serially managed nonreparable as specified in Attachment Number ----.

(iv) Any item of special tooling or special test equipment as defined in FAR 2.101 that have been designated for preservation and storage for a Major Defense Acquisition Program as specified in Attachment Number ----.

(v) Any item not included in paragraphs (c)(1)(i), (ii), (iii), or

(iv) of this clause for which the contractor creates and marks a unique item identifier for traceability.

(2) The unique item identifier assignment and its component data element combination shall not be duplicated on any other item marked or registered in the DoD Item Unique Identification Registry by the contractor.

(3) The unique item identifier component data elements shall be marked on an item using two dimensional data matrix symbology that complies with ISO/IEC International Standard 16022, Information technology--International symbology specification--Data matrix; ECC200 data matrix specification.

(4) Data syntax and semantics of unique item identifiers. The Contractor shall ensure that--

(i) The data elements (except issuing agency code) of the unique item identifier are encoded within the data matrix symbol that is marked on the item using one of the following three types of data qualifiers, as determined by the Contractor: (A) Application Identifiers (AIs) (Format Indicator 05 of ISO/IEC International Standard 15434), in accordance with ISO/IEC International Standard 15418, Information Technology--EAN/UCC Application Identifiers and Fact Data Identifiers and Maintenance and ANSI MH 10.8.2 Data Identifier and Application Identifier Standard.

(B) Data Identifiers (DIs) (Format Indicator 06 of ISO/IEC International Standard 15434), in accordance with ISO/IEC International Standard 15418, Information Technology--EAN/UCC Application Identifiers and Fact Data Identifiers and Maintenance and ANSI MH 10.8.2 Data Identifier and Application Identifier Standard.

(C) Text Element Identifiers (TEIs) (Format Indicator 12 of ISO/IEC International Standard 15434), in accordance

with the Air Transport Association Common Support Data Dictionary; and

(ii) The encoded data elements of the unique item identifier conform to the transfer structure, syntax, and coding of messages and data formats specified for Format Indicators 05, 06, and 12 in ISO/IEC International Standard 15434, Information Technology-Transfer Syntax for High Capacity Automatic Data Capture Media.

(5) Unique item identifier.

(i) The Contractor shall--

(A) Determine whether to--



- (1) Serialize within the enterprise identifier; N/A
  - (2) Serialize within the part, lot, or batch number; or
  - (3) Use a DoD recognized unique identification equivalent (e.g. Vehicle Identification Number); and
  - (B) Place the data elements of the unique item identifier (enterprise identifier; serial number; DoD recognized unique identification equivalent; and for serialization within the part, lot, or batch number only: Original part, lot, or batch number) on items requiring marking by paragraph (c)(1) of this clause, based on the criteria provided in MIL-STD-130, Identification Marking of U.S. Military Property, latest version;
  - (C) Label shipments, storage containers and packages that contain uniquely identified items in accordance with the requirements of MIL-STD-129, Military Marking for Shipment and Storage, latest version; and
  - (D) Verify that the marks on items and labels on shipments, storage containers, and packages are machine readable and conform to the applicable standards. The contractor shall use an automatic identification technology device for this verification that has been programmed to the requirements of Appendix A, MIL-STD-130, latest version.
    - (ii) The issuing agency code--
      - (A) Shall not be placed on the item; and
      - (B) Shall be derived from the data qualifier for the enterprise identifier.
    - (d) For each item that requires item unique identification under paragraph (c)(1)(i), (ii), or (iv) of this clause or when item unique identification is provided under paragraph (c)(1)(v), in addition to the information provided as part of the Material Inspection and Receiving Report specified elsewhere in this contract, the Contractor shall report at the time of delivery, as part of the Material Inspection and Receiving Report, the following information:
      - (1) Unique item identifier.
      - (2) Unique item identifier type.
      - (3) Issuing agency code (if concatenated unique item identifier is used).
      - (4) Enterprise identifier (if concatenated unique item identifier is used).
      - (5) Original part number (if there is serialization within the original part number).
      - (6) Lot or batch number (if there is serialization within the lot or batch number).
      - (7) Current part number (optional and only if not the same as the original part number).
      - (8) Current part number effective date (optional and only if current part number is used).
- W91260-15-D-0003
- Page 62 of 65
- (9) Serial number (if concatenated unique item identifier is used).
  - (10) Government's unit acquisition cost.
  - (11) Unit of measure.
  - (e) For embedded subassemblies, components, and parts that require DoD unique item identification under paragraph (c)(1)(iii) of this clause, the Contractor shall report as part of, or associated with, the Material Inspection and Receiving Report specified elsewhere in this contract, the following information:
    - (1) Unique item identifier of the parent item under paragraph (c)(1) of this clause that contains the embedded subassembly, component, or part.
    - (2) Unique item identifier of the embedded subassembly, component, or part.
    - (3) Unique item identifier type.\*\*

- (4) Issuing agency code (if concatenated unique item identifier is used).\*\*
- (5) Enterprize identifier (if concatenated unique item identifier is used).\*\*
- (6) Original part number (if there is serialization within the original part number).\*\*
- (7) Lot or batch number (if there is serialization within the lot or batch number).\*\*
- (8) Current part number (optional and only if not the same as the original part number).\*\*
- (9) Current part number effective date (optional and only if current part number is used).\*\*
- (10) Serial number (if concatenated unique item identifier is used).\*\*
- (11) Description.
- (12) Type designation of the item as specified in the contract schedule, if any.
- (13) Whether the item is an item of Special Tooling or Special Test Equipment.
- (14) Whether the item is covered by a warranty.

\*\* Once per item.

(e) For embedded subassemblies, components, and parts that require DoD item unique identification under paragraph (c)(1)(iii) of this clause or when item unique identification is provided under paragraph (c)(1)(v), the Contractor shall report as part of the Material Inspection and Receiving Report specified elsewhere in this contract, the following information:

(f) The Contractor shall submit the information required by paragraphs (d) and (e) of this clause as follows:

(1) End items shall be reported using the receiving report capability in Wide Area WorkFlow (WAWF) in accordance with the clause at 252.232-7003. If WAWF is not required by this contract, and the contractor is not using WAWF, follow the procedures at <http://dodprocurementtoolbox.com/site/uidregistry/>.

(2) Embedded items shall be reported by one of the following methods

(i) Use of the embedded items capability in WAWF;

(ii) Direct data submission to the IUID Registry following the procedures and formats at <http://dodprocurementtoolbox.com/site/uidregistry/>; or

(iii) Via WAWF as a deliverable attachment for exhibit line item number (fill in) ----, Unique Item Identifier Report for Embedded Items, Contract Data Requirements List, DD Form 1423.

(g) Subcontracts. If the Contractor acquires by contract any items for which item unique identification is required in accordance with paragraph (c)(1) of this clause, the Contractor shall include this clause, including this paragraph (g), in the applicable subcontract(s), including subcontracts for commercial items.

(End of clause)

#### 252.237-7023 CONTINUATION OF ESSENTIAL CONTRACTOR SERVICES (OCT 2010)

(a) Definitions. As used in this clause-

(1) Essential contractor service means a service provided by a firm or individual under contract to DoD to support mission-essential functions, such as support of vital systems, including ships owned, leased, or operated in support of military missions or roles at sea; associated support activities, including installation,

garrison, and base support services; and similar services provided to foreign military sales customers under the Security Assistance Program. Services are essential if the effectiveness of defense systems or operations has the potential to be seriously impaired by the interruption of these services, as determined by the appropriate functional commander or civilian equivalent.

(2) Mission-essential functions means those organizational activities that must be performed under all circumstances to achieve DoD component missions or responsibilities, as determined by the appropriate functional commander or civilian equivalent. Failure to perform or sustain these

functions would significantly affect DoD's ability to provide vital services or exercise authority, direction, and control.

(b) The Government has identified all or a portion of the contractor services performed under this contract as essential contractor services in support of mission-essential functions. These services will be identified in the applicable task order.

(c)(1) The Mission-Essential Contractor Services Plan submitted by the Contractor, is incorporated in this contract.

(2) The Contractor shall maintain and update its plan as necessary. The Contractor shall provide all plan updates to the Contracting Officer for approval.

(3) As directed by the Contracting Officer, the Contractor shall participate in training events, exercises, and drills associated with Government efforts to test the effectiveness of continuity of operations procedures and practices.

(d)(1) Notwithstanding any other clause of this contract, the Contractor shall be responsible to perform those services identified as essential contractor services during crisis situations (as directed by the Contracting Officer), in accordance with its Mission-Essential Contractor Services Plan.

(2) In the event the Contractor anticipates not being able to perform any of the essential contractor services identified in accordance with paragraph (b) of this clause during a crisis situation, the Contractor shall notify the Contracting Officer or other designated representative as expeditiously as possible and use its best efforts to cooperate with the Government in the Government's efforts to maintain the continuity of operations.

(e) The Government reserves the right in such crisis situations to use Federal employees, military personnel, or contract support from other contractors, or to enter into new contracts for essential contractor services.

(f) Changes. The Contractor shall segregate and separately identify all costs incurred in continuing performance of essential services in a crisis situation. The Contractor shall notify the Contracting Officer of an increase or decrease in costs within ninety days after continued performance has been directed by the Contracting Officer, or within any additional period that the Contracting Officer approves in writing, but not later than the date of final payment under the contract. The Contractor's notice shall include the Contractor's proposal for an equitable adjustment and any data supporting the increase or decrease in the form prescribed by the Contracting Officer. The parties shall negotiate an equitable price adjustment to the contract price, delivery schedule, or both as soon as is practicable after receipt of the Contractor's proposal.

(g) The Contractor shall include the substance of this clause, including this paragraph (g), in subcontracts for the essential services.

(End of clause)