Additional General Provisions For Projects 524012, 524019 and 524020

The following articles supersede the supplemental clauses incorporated in Section 37.0 of SCM-TMP-002 and Section 38.0 of SCM-TMP-005. All other provisions of the applicable document for this order are incorporated and available at https://gdmissionsystems.com/about-us/suppliers/terms-and-conditions.

Articles Applicable to This Order Irrespective of the Amount of the Order

ANTI-KICKBACK PROCEDURES

A. Definitions.

Kickback, as used in this article, means any money, fee, commission, credit, gift, gratuity, thing of value, or compensation of any kind which is provided to any prime Contractor, prime Contractor employee, subcontractor, or subcontractor employee for the purpose of improperly obtaining or rewarding favorable treatment in connection with a prime contract or in connection with a subcontract relating to a prime contract.

Person, as used in this article, means a corporation, partnership, business association of any kind, trust, joint-stock company, or individual.

Prime Agreement, as used in this article, means any Agreement entered into by the United States for the purpose of obtaining supplies, materials, equipment, for use within the program.

Prime Contractor as used in this article, means a person who has entered into a Prime Agreement with the United States.

Prime Contractor employee, as used in this article, means any officer, partner, employee, or agent of a prime Contractor.

Subcontract, as used in this article, means a contract or contractual action entered into by a prime Contractor or subcontractor for the purpose of obtaining supplies, materials, or equipment, under the Prime Agreement in support of the program.

Subcontractor, as used in this article, means any person, other than the prime Contractor, who offers to furnish or furnishes any supplies, materials, or equipment, under the Prime Agreement or a subcontract entered into in connection with such Prime Agreement, and includes any person who offers to furnish or furnishes general supplies to the prime Contractor or a higher tier subcontractor.

Subcontractor employee, as used in this article, means any officer, partner, employee, or agent of a subcontractor.

B. 41 U.S.C. chapter 87, Kickbacks, prohibits any person from-

1. Providing or attempting to provide or offering to provide any kickback;
2. Soliciting, accepting, or attempting to accept any kickback; or
3. Including, directly or indirectly, the amount of any kickback in the Agreement price charged by a prime Contractor to the United States or in the Agreement price charged by a subcontractor to a prime Contractor or higher tier subcontractor.

Additional General Provisions For Projects 524012, 524019 and 524020

C.

1. When the Contractor has reasonable grounds to believe that a violation described in paragraph (B) of this article may have occurred, the Contractor shall promptly report in writing the possible violation within one calendar week (7 days). Such reports shall be made to the inspector general of the AF contracting agency, the AF Inspector General, or the Attorney General.

2. The Contractor shall cooperate fully with any Federal agency investigating a possible violation described in paragraph (B) of this clause.

3. The Agreement Officer may offset the amount of the kickback against any monies owed by the United States under the Prime Agreement and/or direct that the Prime Contractor withhold from sums owed a subcontractor under the Prime Agreement the amount of the kickback. The Agreement Officer may order that monies withheld under subdivision (C)(3) of this article be paid over to the Government unless the Government has already offset those monies under subdivision (C)(3) of this article. In either case, the Prime Contractor shall notify the Agreement Officer when the monies are withheld.

4. The Contractor agrees to incorporate the substance of this article in all subcontracts under this Agreement.

PROHIBITION REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS

A. Definitions. As used in this article-

1. Internal confidentiality agreement or statement means a confidentiality agreement or any other written statement that the contractor requires any of its employees or subcontractors to sign regarding nondisclosure of contractor information, except that it does not include confidentiality agreements arising out of civil litigation or confidentiality agreements that contractor employees or subcontractors sign at the behest of a Federal agency.

2. Subcontract is defined as any contract or agreement entered into by a subcontractor to furnish supplies or services for performance of a prime contract or agreement or a subcontract. It includes but is not limited to purchase orders, and changes and modifications to purchase orders.

3. Subcontractor means any supplier, distributor, vendor, or firm (including a consultant) that furnishes supplies or services to or for a prime contractor or another subcontractor.

B. The Contractor shall not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

C. The Contractor shall notify current employees and subcontractors that prohibitions and restrictions of any preexisting internal confidentiality agreements or statements covered by this clause, to the extent that such prohibitions and restrictions are inconsistent with the prohibitions of this clause, are no longer in effect.

Additional General Provisions For Projects 524012, 524019 and 524020

D. The prohibition in paragraph (D) of this article does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

E. In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015, (Pub. L. 113-235), and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions) use of funds appropriated (or otherwise made available) is prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this article.

F. The Contractor shall include the substance of this article in subcontracts under this Agreement.

COMPLIANCE WITH SECTION 889 OF NDAA FY19

A. Definitions. As used in this article-

1. 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).

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

3. Covered telecommunications equipment or services means-

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

b. 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);

c. Telecommunications or video surveillance services provided by such entities or using such equipment; or

d. 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.

4. Critical technology means-

a. 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;

b. 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-

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

2. For reasons relating to regional stability or surreptitious listening;

c. 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);

d. 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);

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

5. 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.

6. 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.

7. 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.

8. 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.

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 Agreement 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 Agreement 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 Agreements Officer for the indefinite delivery contract and the Contracting or Agreements 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 article

a. Within one business day from the date of such identification or notification: the contract number; agreement 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.

b. Within ten (10) business days of submitting the information in paragraph (d)(2)(a) of this article: 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.

1. The Contractor shall insert the substance of this article in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

Additional General Provisions For Projects 524012, 524019 and 524020

RESTRICTIONS ON CERTAIN FOREIGN PURCHASES

A. Except as authorized by the Office of Foreign Assets Control (OFAC) in the Department of the Treasury, the Contractor shall not acquire, for use in the performance of this Agreement, any supplies or services if any proclamation, Executive order, or statute administered by OFAC, or if OFAC's implementing regulations at 31 CFR Chapter V, would prohibit such a transaction by a person subject to the jurisdiction of the United States.

B. Except as authorized by OFAC, most transactions involving Cuba, Iran, and Sudan are prohibited, as are most imports from Burma or North Korea, into the United States or its outlying areas. Lists of entities and individuals subject to economic sanctions are included in OFAC's List of Specially Designated Nationals and Blocked Persons at https://sanctionssearch.ofac.treas.gov/. More information about these restrictions, as well as updates, is available in the OFAC's regulations at 31 CFR Chapter V and/or on OFAC's website at https://home.treasury.gov/policy-issues/financial-sanctions/additional-ofacresources/ofac-legal-library/code-of-federal-regulations-cfr.

C. The Contractor shall insert this article in all subcontracts.

SAFEGUARDING COVERED DEFENSE INFORMATION & CYBER INCIDENT REPORTING

A. Definitions. As used in this article-

1. "Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

2. "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.

3. "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.

4. "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.

5. "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.

Additional General Provisions For Projects 524012, 524019 and 524020

6. “Covered defense information” means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/category-list.html>, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is

a. Marked or otherwise identified in the Agreement and provided to the contractor by or on behalf of DoD in support of the performance of the Agreement; or

b. Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the Agreement.

7. “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.

8. “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.

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

10. “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.

11. “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.

12. ‘‘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.

13. “Rapidly report” means within seventy-two (72) hours of discovery of any cyber incident.

14. “Technical information” means technical data or computer software.

15. “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 administration, such as financial and/or management information.

16. “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.

17. Noncommercial Items, regardless of whether or not the article is incorporated in this solicitation or Agreement. 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.

1. 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:

a. 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:

1. Cloud computing services shall be subject to the security requirements specified in DFARS clause 252.239-7010 <https://www.acquisition.gov/dfars/part-252-clauses> , Cloud Computing Services.

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

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 article, the following security requirements apply:

a. Except as provided in paragraph (B)(2)(b) of this article, 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 Agreement Officer.

b.

1. The Contractor shall implement NIST SP 800-171.

2. The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Agreement 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 non-applicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

3. 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 Agreement Officer when requesting its recognition under this Agreement.

4. If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this Agreement, 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/> and that the cloud service provider complies with requirements in paragraphs (C) through (G) of this article 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.

5. 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 article, 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 Agreement that are designated as operationally critical support and identified in the Agreement, the Contractor shall.

a. 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

b. Rapidly report cyber incidents to DoD at <https://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 <https://dibnet.dod.mil>.

3. Medium assurance certificate requirement. In order to report cyber incidents in accordance with this article, 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 <https://public.cyber.mil/eca/>.

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 Agreement Officer. Do not send the malicious software to the Agreement 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)(a) of this article and all relevant monitoring/packet capture data for at least ninety (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 Agreement Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (F) of this article.

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 article 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.

1. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this article that is not created by or for DoD is authorized to be released outside of DoD-

a. To entities with missions that may be affected by such information;

b. To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

c. To Government entities that conduct counterintelligence or law enforcement investigations;

d. 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

e. To a support services contractor ("recipient") that is directly supporting Government activities under this Agreement that includes DFARS clause at 252.204-7009 <https://www.acquisition.gov/dfars/part-252-clauses> , 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 article that is created by or for DoD (including the information submitted pursuant to paragraph (C) of this article) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this article, and for any other lawful Government purpose or activity, subject to all applicable statutory, FA8735-21-9-0001PAGE 48 OF 56 regulatory, and policy based restrictions on the Government's use and release of such information.

K. The Contractor shall conduct activities under this article 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 article 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 articles of this Agreement, or as a result of other applicable U.S. Government statutory or regulatory requirements.

M. Subcontracts.

The Contractor shall-

1. Include this article 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 article, and, if necessary, consult with the Agreement Officer; and

2. Require subcontractors to-

a. 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 Agreement Officer, in accordance with paragraph (B)(2)(b) of this article; and

b. 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 article.

Additional General Provisions For Projects 524012, 524019 and 524020

Articles Applicable If This Order Exceeds $250,000

RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT

A. Except as provided in (B) of this article, the Contractor shall not enter into any agreement with an actual or prospective subcontractor, nor otherwise act in any manner, which has or may have the effect of restricting sales by such subcontractors directly to the Government of any item or process (including computer software) made or furnished by the subcontractor under this Agreement or under any follow-on Agreement or contract.

B. The prohibition in (A) of this article does not preclude the Contractor from asserting rights that are otherwise authorized by law or regulation.

WHISTLEBLOWER RIGHTS

A. This Agreement and employees working on this Agreement will be subject to the whistleblower rights and remedies in the pilot program on Contractor employee whistleblower protections established at 41 U.S.C. 4712 by section 828 of the National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112-239).

B. The Contractor shall inform its employees in writing, in the predominant language of the workforce, of employee whistleblower rights and protections under 41 U.S.C. 4712.

C. The Contractor shall insert the substance of this article, including this paragraph (C), in all subcontracts over the simplified acquisition threshold.

EQUAL EMPLOYMENT OPPORTUNITY FOR VETERANS

A. Equal opportunity article. The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60-300.5(a), as of March 24, 2014. This article prohibits discrimination against qualified protected veterans, and requires affirmative action by the Contractor to employ and advance in employment qualified protected veterans.

B. Subcontracts. The Contractor shall insert the terms of this article in subcontracts valued at or above the simplified acquisition threshold on the date of subcontract award, unless exempted by rules, regulations, or orders of the Secretary of Labor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate to identify properly the parties and their undertakings.