ITES-3S CONTRACT NO. W52P1J-18-D-A061
PRIME CONTRACT FLOWDOWNS

BETWEEN

SUBCONTRACTOR
(Also Referred to as **Subcontractor, Offeror** or **Seller**)

AND

Iron Bow Technologies, LLC
2121 Cooperative Way, Suite 500
Herndon, VA 20171
(Also Referred to as **Prime Contractor** or **Buyer**)

WHERE THE WORDS "CONTRACTING OFFICER" AND "CONTRACTOR" APPEAR IN THE TEXT OF SUCH PROVISIONS, SUCH REFERENCE SHALL MEAN "IRON BOW" AND "SUBCONTRACTOR" RESPECTIVELY. REFERENCES IN SUCH PROVISIONS TO THE "GOVERNMENT" SHALL REMAIN AS STATED EXCEPT WHERE IT IS CLEAR THAT "IRON BOW" SHOULD BE SUBSTITUTED ACCORDINGLY. ALL REFERENCES IN SUCH PROVISIONS TO "CONTRACT" SHALL MEAN THIS SUBCONTRACT. ADDITIONAL OR DIFFERING TERMS, CONDITIONS OR LIMITATIONS OF LIABILITY PROPOSED BY SELLER, WHETHER IN A QUOTE, ACCEPTANCE OR DELIVERY DOCUMENT SHALL HAVE NO EFFECT UNLESS ACCEPTED IN WRITING BY BUYER. IN PARTICULAR, ANY LIMITATION OF LIABILITY OR DISCLAIMER OF WARRANTY IS EXPRESSLY REJECTED.

ALL DELIVERY ORDERS/EFFORTS AWARDED UNDER ITES-3S SHOULD BE TREATED AS HAVING A **DPAS RATING OF DOA7, BASED ON THE MASTER CONTRACT. THE 3S DO/TASK ORDER SHOULD BE GIVEN PRIORITY OVER OTHER CONTRACTS, OR ORDERS AGAINST OTHER CONTRACTS, WITH LOWER OR NO RATING.**

SECTION E - INSPECTION AND ACCEPTANCE

	Regulatory Cite	Title	Date
E-1	52.246-2	INSPECTION OF SUPPLIES--FIXED-PRICE	AUG/1996
E-2	52.246-3	INSPECTION OF SUPPLIES--COST-REIMBURSEMENT	MAY/2001
E-3	52.246-4	INSPECTION OF SERVICES--FIXED-PRICE	AUG/1996
E-4	52.246-5	INSPECTION OF SERVICES--COST-REIMBURSEMENT	APR/1984
E-5	52.246-6	INSPECTION--TIME-AND-MATERIAL AND LABOR-HOUR	MAY/2001
E-6	52.246-12	INSPECTION OF CONSTRUCTION	AUG/1996
E-7	52.246-13	INSPECTION--DISMANTLING, DEMOLITION, OR REMOVAL OF IMPROVEMENTS	AUG/1996
E-8	52.246-15	CERTIFICATE OF CONFORMANCE	APR/1984
E-9	52.246-16	RESPONSIBILITY FOR SUPPLIES	APR/1984

SECTION F - DELIVERIES OR PERFORMANCE

	Regulatory Cite	Title	Date
F-1	52.242-15	STOP-WORK ORDER	AUG/1989
F-2	52.242-17	GOVERNMENT DELAY OF WORK	APR/1984
F-3	252.211-7007	REPORTING OF GOVERNMENT-FURNISHED PROPERTY	AUG/2012
F-4	252.211-7003	ITEM UNIQUE IDENTIFICATION AND VALUATION	MAR/2016

SECTION H - SPECIAL CONTRACT REQUIREMENTS

	Regulatory Cite	Title	Date
H-1	252.222-7006	RESTRICTIONS ON THE USE OF MANDATORY ARBITRATION AGREEMENTS	DEC/2010

1. As defined in Army Regulation (AR) 530-1, Operations Security (OPSEC), sensitive information is information requiring special protection from disclosure that could cause compromise or threat to our national security, an Army organization, activity, family member, DA civilian or DoD contractor. Critical Information is defined as information important to the successful achievement of U.S. objectives and missions, or which may be of use to an adversary of the United States. It consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and intentions needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment. All critical information is sensitive, but not all sensitive information is critical.

2. The Contractor shall not release sensitive information to the general public without prior written approval from the Contracting Officer. All contractor requests to release sensitive information shall be in writing and clearly explain the necessity for release of the information and consequences if approval is not granted. Contractor employees who are U.S. citizens shall be provided access to sensitive information on a "need to know" basis required to fulfill the terms and conditions of the contract. Foreign National (FN) employees access to information will be limited to non-sensitive information. FN access to sensitive information will be approved in writing by the Contracting Officer on a case-by-case basis, and will be strictly limited to the information that the employee must know in order to fulfill the terms and conditions of the contract.

3. The Contracting Officer will provide the Contractor with a list of known Critical Information (CI) pertinent to contract requirements and threat information pertinent to contract location as soon as possible after contract award. Critical Information and threat information shall be used by the Contractors appointed OPSEC Manager to prepare an OPSEC Plan.

4. The Contractor shall be responsible for establishing and maintaining an OPSEC program to adequately manage, protect and control sensitive information that has been provided or generated under the contract. The Contractor shall prepare and submit a written OPSEC Plan to the Contracting Officer for approval IAW DD 1423/DI-MGMT-80934C within 30 calendar days after receipt of the CI/threat information addressed in Paragraph 3 above. The Contracting Officer will coordinate with the Government OPSEC Officer and advise the Contractor in writing of the approval, conditional approval or disapproval of the plan within 10 days of receipt.

5. The Contractor shall conduct annual self-assessments of their OPSEC program and submit annual written assessments to the Contracting Officer in the anniversary month of contract award. OPSEC Assessment checklists and sample assessment responses will be provided in advance by the Government as tools to aid the Contractor in assessing their OPSEC program.

6. The Contractor shall provide OPSEC training to all employees regarding the safeguarding of sensitive information prior to employees being allowed access to such information, and annually thereafter.

7. The Contractor shall destroy all sensitive program material at the completion of the contract so as to ensure the information cannot be accessed or utilized for any purpose and notify the Contracting Officer in writing of its destruction.

8. These same requirements will flow down to all subcontractors working on or provided any sensitive information related to the contract.

(End of Clause)

I-182 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS JUL/2018

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015)
(2) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).
(3) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless

otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(ii) 52.219-8, Utilization of Small Business Concerns (OCT 2014) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $700,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iii) 52.222-17, Nondisplacement of Qualified Workers (MAY 2014) (E.O. 13495). Flow down required in accordance with paragraph (l) of FAR clause 52.222-17.

(iv) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(v) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).

(vi) 52.222-35, Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (Oct 2015)(38 U.S.C. 4212).

(vii) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014)(29 U.S.C. 793).

(viii) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).

(ix) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).

(x) 52.222-41, Service Contract Labor Standards (MAY 2014) (41 U.S.C. chapter 67).

(xi) 52.222-50, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. 7104(g)).
___ Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. 7104(g)).

(xii) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xiii) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services—Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xiv) 52.222-54, Employment Eligibility Verification (Oct 2015).

(xv) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015) (Executive Order 13658).

(xvi) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Jul 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xvii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (MAY 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xviii) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

I-1 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT AUG/2019

I-188 52.217-8 OPTION TO EXTEND SERVICES NOV/1999

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may
exercise the option by written notice to the Contractor within not less than 30 days before the expiration of the contract.

(End of Clause)

I-189 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT MAR/2000

(a) The Government may extend the term of this contract by written notice to the Contractor within the term of the contract; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 9 years.

(End of Clause)

I-195 52.246-20 WARRANTY OF SERVICES MAY/2001

(a) Definitions.
Acceptance, as used in this clause, means the act of an authorized representative of the Government by which the Government assumes for itself, or as an agent of another, ownership of existing and identified supplies, or approves specific services, as partial or complete performance of the contract.

(b) Notwithstanding inspection and acceptance by the Government or any provision concerning the conclusiveness thereof, the Contractor warrants that all services performed under this contract will, at the time of acceptance, be free from defects in workmanship and conform to the requirements of this contract. The Contracting Officer shall give written notice of any defect or nonconformance to the Contractor [For Base Contract: Not Applicable. For Task Orders: OCO to insert specific period of time in which notice shall be given to the Contractor; e.g. "within 30 days from the date of acceptance by the Government", "within 1000 hours of use by the Government"; or other specific event whose occurrence will terminate the period of notice, or combination of any applicable event or period of time.]

This notice shall state either –

(1) That the Contractor shall correct or re-perform any defective or nonconforming services; or

(2) That the Government does not require correction or re-performance.

(c) If the Contractor is required to correct or re-perform, it shall be at no cost to the Government, and any services corrected or Re-performed by the Contractor shall be subject to this clause to the same extent as work initially performed. If the Contractor fails or refuses to correct or re-perform, the Contracting Officer may, by contract or otherwise, correct or replace with similar services and charge to the Contractor the cost occasioned to the Government thereby, or make an equitable adjustment in the contract price.

(d) If the Government does not require correction or re-performance, the Contracting Officer shall make an equitable adjustment in the contract price.

(End of Clause)

I-198 252.225-7043 ANTITERRORISM/FORCE PROTECTION POLICY FOR DEFENSE CONTRACTORS OUTSIDE THE UNITED STATES JUN/2015

(a) Definition. United States, as used in this clause, means, the 50 States, the District of Columbia, and outlying areas.

(b) Except as provided in paragraph (c) of this clause, the Contractor and its subcontractors, if performing or traveling outside the United States under this contract, shall

(1) Affiliate with the Overseas Security Advisory Council, if the Contractor or subcontractor is a U.S. entity;

(2) Ensure that Contractor and subcontractor personnel who are U.S. nationals and are in-country on a non-transitory basis, register with the U.S. Embassy, and that Contractor and subcontractor personnel who are third country nationals comply with any security related requirements of the Embassy of their nationality;

(3) Provide, to Contractor and subcontractor personnel, antiterrorism/force protection awareness information commensurate with that which the Department of Defense (DoD) provides to its military and civilian personnel and their families, to the extent such information can be made available prior to travel outside the United States; and

(4) Obtain and comply with the most current antiterrorism/force protection guidance for Contractor and subcontractor personnel.

(c) The requirements of this clause do not apply to any subcontractor that is:

(1) A foreign government;

(2) A representative of a foreign government; or

(3) A foreign corporation wholly owned by a foreign government.

(d) Information and guidance pertaining to DoD antiterrorism/force protection can be obtained from -1-.

(End of clause)

I-199 252.237-7019 TRAINING FOR CONTRACTOR PERSONNEL INTERACTING WITH DETAINEES JUN/2013

(a) Definitions. As used in this clause

Combatant Commander means the commander of a unified or specified combatant command established in accordance with 10 U.S.C. 161.

Detainee means a person in the custody or under the physical control of the Department of Defense on behalf of the United States Government as a result of armed conflict or other military operation by United States armed forces.

Personnel interacting with detainees means personnel who, in the course of their duties, are expected to interact with detainees.

(b) Training requirement. This clause implements Section 1092 of the National Defense Authorization Act for Fiscal Year 2005 (Pub. L. 108-375).

(1) The Combatant Commander responsible for the area where a detention or interrogation facility is located will arrange for training to be provided to contractor personnel interacting with detainees. The training will address the international obligations and laws of the United States applicable to the detention of personnel, including the Geneva Conventions. The Combatant Commander will arrange for a training receipt document to be provided to personnel who have completed the training.

(2)(i) The Contractor shall arrange for its personnel interacting with detainees to

(A) Receive the training specified in paragraph (b)(1) of this clause
(1) Prior to interacting with detainees, or as soon as possible if, for compelling reasons, the Contracting Officer authorizes interaction with detainees prior to receipt of such training; and

(2) Annually thereafter; and
(B) Provide a copy of the training receipt document specified in paragraph (b)(1) of this clause to the Contractor for retention.

(ii) To make these arrangements, the following points of contact apply:

[For Base Contract: Not Applicable. For Task Orders: OCO to insert applicable point of contact information cited in DFARS PGI 237.171-4, as applicable.]

(3) The Contractor shall retain a copy of the training receipt document(s) provided in accordance with paragraphs (b)(1) and (2) of this clause until the contract is closed, or 3 years after all work required by the contract has been completed and accepted by the Government, whichever is sooner.

(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in all subcontracts, including subcontracts for commercial items, that may require subcontractor personnel to interact with detainees in the course of their duties.

(End of clause)

I-200 252.237-7023 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 are listed in attachment [For Base Contract: Not applicable. For Task Orders: OCO to provide location of attachment listing mission essential services as submitted by the requiring agency], Mission-Essential Contractor Services, dated [For Base Contract: Not applicable. For Task Orders: OCO to identify the date of the relevant attachment].

(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)

I-201 252.239-7016 TELECOMMUNICATIONS SECURITY EQUIPMENT, DEVICES, TECHNIQUES, AND SERVICES DEC/1991

(a) Definitions. As used in this clause

(1) Securing means the application of Government-approved telecommunications security equipment, devices, techniques, or services to contractor telecommunications systems.

(2) Sensitive information means any information the loss, misuse, or modification of which, or unauthorized access to, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. 552a (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or Act of Congress to be kept secret in the interest of national defense or foreign policy.

(3) Telecommunications systems means voice, record, and data communications, including management information systems and local data networks that connect to external transmission media, when employed by Government agencies, contractors, and subcontractors to transmit

(i) Classified or sensitive information;

(ii) Matters involving intelligence activities, cryptologic activities related to national security, the command and control of military forces, or equipment that is an integral part of a weapon or weapons system; or

(iii) Matters critical to the direct fulfillment of military or intelligence missions.

(b) This solicitation/contract identifies classified or sensitive information that requires securing during telecommunications and requires the Contractor to secure telecommunications systems. The Contractor agrees to secure information and systems at the following location: [For Base Contract: Not Applicable. For Task Orders: To be determined by OCO, if applicable.]

(c) To provide the security, the Contractor shall use Government-approved telecommunications equipment, devices, techniques, or services. A list of the approved equipment, etc. may be obtained from [For Base Contract: Not Applicable. For Task Orders: To be determined by OCO, if applicable]. Equipment, devices, techniques, or services used by the Contractor must be compatible or

interoperable with [For Base Contract: Not Applicable. For Task Orders: To be determined by OCO, if applicable].

(d) Except as may be provided elsewhere in this contract, the Contractor shall furnish all telecommunications security equipment, devices, techniques, or services necessary to perform this contract. The Contractor must meet ownership eligibility conditions for communications security equipment designated as controlled cryptographic items.

(e) The Contractor agrees to include this clause, including this paragraph (e), in all subcontracts which require securing telecommunications.

(End of clause)

I-203 52.203-13 CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT OCT/2015

(a) Definitions. As used in this clause--
"Agent" means any individual, including a director, an officer, an employee, or an independent Contractor, authorized to act on behalf of the organization.

"Full cooperation"—

(1) Means disclosure to the Government of the information sufficient for law enforcement to identify the nature and extent of the offense and the individuals responsible for the conduct. It includes providing timely and complete response to Government auditors and investigators' request for documents and access to employees with information;

(2) Does not foreclose any Contractor rights arising in law, the FAR, or the terms of the contract. It does not require—

(i) A Contractor to waive its attorney-client privilege or the protections afforded by the attorney work product doctrine; or

(ii) Any officer, director, owner, or employee of the Contractor, including a sole proprietor, to waive his or her attorney client privilege or Fifth Amendment rights; and

(3) Does not restrict a Contractor from--

(i) Conducting an internal investigation; or

(ii) Defending a proceeding or dispute arising under the contract or related to a potential or disclosed violation.

"Principal" means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).

"Subcontract" means any contract entered into by a subcontractor to furnish supplies or services for performance of a prime contract or a subcontract.

"Subcontractor" means any supplier, distributor, vendor, or firm that furnished supplies or services to or for a prime contractor or another subcontractor.

"United States," means the 50 States, the District of Columbia, and outlying areas.

(b) Code of business ethics and conduct.
(1) Within 30 days after contract award, unless the Contracting Officer establishes a longer time period, the Contractor shall--
(i) Have a written code of business ethics and conduct; and

(ii) Make a copy of the code available to each employee engaged in performance of the contract.
(2) The Contractor shall—

(i) Exercise due diligence to prevent and detect criminal conduct; and

(ii) Otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

(3)(i) The Contractor shall timely disclose, in writing, to the agency Office of the Inspector General (OIG), with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed—

(A) A violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code; or

(B) A violation of the civil False Claims Act (31 U.S.C. 3729-3733).

(ii) The Government, to the extent permitted by law and regulation, will safeguard and treat information obtained pursuant to the Contractors disclosure as confidential where the information has been marked confidential or proprietary by the company. To the extent permitted by law and regulation, such information will not be released by the Government to the public pursuant to a Freedom of Information Act request, 5 U.S.C. Section 552, without prior notification to the Contractor. The Government may transfer documents provided by the Contractor to any department or agency within the Executive Branch if the information relates to matters within the organizations jurisdiction.

(iii) If the violation relates to an order against a Government-wide acquisition contract, a multi-agency contract, a multiple-award schedule contract such as the Federal Supply Schedule, or any other procurement instrument intended for use by multiple agencies, the Contractor shall notify the OIG of the ordering agency and the IG of the agency responsible for the basic contract.

(c) Business ethics awareness and compliance program and internal control system. This paragraph (c) does not apply if the Contractor has represented itself as a small business concern pursuant to the award of this contract or if this contract is for the acquisition of a commercial item as defined at FAR 2.101. The Contractor shall establish the following within 90 days after contract award, unless the Contracting Officer establishes a longer time period:

(1) An ongoing business ethics awareness and compliance program.

(i) This program shall include reasonable steps to communicate periodically and in a practical manner the Contractors standards and procedures and other aspects of the Contractors business ethics awareness and compliance program and internal control system, by conducting effective training programs and otherwise disseminating information appropriate to an individual's respective roles and responsibilities.

(ii) The training conducted under this program shall be provided to the Contractors principals and employees, and as appropriate, the Contractors agents and subcontractors.

(2) An internal control system.

(i) The Contractors internal control system shall—

(A) Establish standards and procedures to facilitate timely discovery of improper conduct in connection with Government contracts; And

(B) Ensure corrective measures are promptly instituted and carried out.

(ii) At a minimum, the Contractors internal control system shall provide for the following:

(A) Assignment of responsibility at a sufficiently high level and adequate resources to ensure effectiveness of the business ethics awareness and compliance program and internal control system.

(B) Reasonable efforts not to include an individual as a principal, whom due diligence would have exposed as having engaged in conduct that is in conflict with the Contractors code of business ethics and conduct.

(C) Periodic reviews of company business practices, procedures, policies, and internal controls for compliance with the Contractors code of business ethics and conduct and the special requirements of Government contracting, including--

(1) Monitoring and auditing to detect criminal conduct;

(2) Periodic evaluation of the effectiveness of the business ethics awareness and compliance program and internal control system, especially if criminal conduct has been detected; and

(3) Periodic assessment of the risk of criminal conduct, with appropriate steps to design, implement, or modify the business
ethics awareness and compliance program and the internal control system as necessary to reduce the risk of criminal conduct identified through this process.

(D) An internal reporting mechanism, such as a hotline, which allows for anonymity or confidentiality, by which employees may report suspected instances of improper conduct, and instructions that encourage employees to make such reports.

(E) Disciplinary action for improper conduct or for failing to take reasonable steps to prevent or detect improper conduct.

(F) Timely disclosure, in writing, to the agency OIG, with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of any Government contract performed by the Contractor or a subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 U.S.C. or a violation of the civil False Claims Act (31 U.S.C. 3729-3733).

(1) If a violation relates to more than one Government contract, the Contractor may make the disclosure to the agency OIG and Contracting Officer responsible for the largest dollar value contract impacted by the violation.

(2) If the violation relates to an order against a Government-wide acquisition contract, a multi-agency contract, a multiple award schedule contract such as the Federal Supply Schedule, or any other procurement instrument intended for use by multiple agencies, the contractor shall notify the OIG of the ordering agency and the IG of the agency responsible for the basic contract, and the respective agencies contracting officers.

(3) The disclosure requirement for an individual contract continues until at least 3 years after final payment on the contract.

(4) The Government will safeguard such disclosures in accordance with paragraph (b)(3)(ii) of this clause.

(G) Full cooperation with any Government agencies responsible for audits, investigations, or corrective actions.

(d) Subcontracts.

(1) The Contractor shall include the substance of this clause, including this paragraph (d), in subcontracts that have a value in excess of $5,500,000 and a performance period of more than 120 days.

(2) In altering this clause to identify the appropriate parties, all disclosures of violation of the civil False Claims Act or of Federal criminal law shall be directed to the agency Office of the Inspector General, with a copy to the

Contracting Officer.

(End of clause)

I-205 52.215-19 NOTIFICATION OF OWNERSHIP CHANGES OCT/1997

(a) The Contractor shall make the following notifications in writing:

(1) When the Contractor becomes aware that a change in its ownership has occurred, or is certain to occur, that could result in changes in the valuation of its capitalized assets in the accounting records, the Contractor shall notify the Administrative Contracting Officer (ACO) within 30 days.

(2) The Contractor shall also notify the ACO within 30 days whenever changes to asset valuations or any other cost changes have occurred or are certain to occur as a result of a change in ownership.

(b) The Contractor shall --

(1) Maintain current, accurate, and complete inventory records of assets and their costs;

(2) Provide the ACO or designated representative ready access to the records upon request;

(3) Ensure that all individual and grouped assets, their capitalized values, accumulated depreciation or amortization, and remaining useful lives are identified accurately before and after each of the Contractors ownership changes; and

(4) Retain and continue to maintain depreciation and amortization schedules based on the asset records maintained before each Contractor ownership change.

(c) The Contractor shall include the substance of this clause in all subcontracts under this contract that meet the applicability requirement of FAR 15.408(k).

(End of Clause)

I-209 52.222-35 EQUAL OPPORTUNITY FOR VETERANS OCT/2015

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

"Active duty wartime or campaign badge veteran," "Armed Forces service medal veteran," "disabled veteran," "protected veteran," "qualified disabled veteran," and "recently separated veteran" have the meanings given at FAR 22.1301.

(b) Equal opportunity clause. 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 clause prohibits discrimination against qualified protected veterans, and requires affirmative action by the Contractor to employ and advance in employment qualified protected veterans.

(c) Subcontracts. The Contractor shall insert the terms of this clause in subcontracts of $150,000 or more 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.

(End of clause)

I-210 52.222-36 EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES JUL/2014

(a) Equal opportunity clause. The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60-741.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified individuals on the basis of disability, and requires affirmative action by the Contractor to employ and advance in employment qualified individuals with disabilities.

(b) Subcontracts. The Contractor shall include the terms of this clause in every subcontract or purchase order in excess of $15,000 unless exempted by rules, regulations, or orders of the Secretary, so that such provisions will be binding upon each subcontractor or vendor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs of the U.S. Department of Labor, 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.

(End of clause)

I-211 52.230-2 COST ACCOUNTING STANDARDS OCT/2015

(a) Unless the contract is exempt under 48 CFR 9903.201-1 and 9903.201-2, the provisions of 48 CFR Part 9903 are incorporated herein by reference and the Contractor, in connection with this contract, shall

(1) (CAS-covered Contracts Only) By submission of a Disclosure Statement, disclose in writing the Contractors cost accounting practices as required by 48 CFR 9903.202-1 through 9903.202-5, including methods of distinguishing direct costs from indirect costs and the basis used for allocating indirect costs. The practices disclosed for this contract shall be the same as the practices currently disclosed and applied on all other contracts and subcontracts being performed by the Contractor and which contain a Cost Accounting Standards (CAS) clause. If the Contractor has notified the Contracting Officer that the Disclosure Statement contains trade secrets and commercial or financial information which is privileged and confidential, the Disclosure Statement shall be protected and shall not be released outside of the Government.

(2) Follow consistently the Contractors cost accounting practices in accumulating and reporting contract performance cost data concerning this contract. If any change in cost accounting practices is made for the purposes of any contract or subcontract subject to CAS requirements, the change must be applied prospectively to this contract and the Disclosure Statement must be amended accordingly. If the contract price or cost allowance of this contract is affected by such changes, adjustment shall be made in accordance with paragraph (a)(4) or (a)(5) of this clause, as appropriate.

(3) Comply with all CAS, including any modifications and interpretations indicated thereto contained in 48 CFR Part 9904, in effect on the date of award of this contract or, if the Contractor has submitted certified cost or pricing data, on the date of final agreement on price as shown on the Contractors signed certificate of current cost or pricing data. The Contractor shall also comply with any CAS (or modifications to CAS) which hereafter become applicable to a contract or subcontract of the Contractor. Such compliance shall be required prospectively from the date of applicability to such contract or subcontract.

(4)(i) (Agree to an equitable adjustment as provided in the Changes clause of this contract if the contract cost is affected by a change which, pursuant to paragraph (a)(3) of this clause, the Contractor is required to make to the Contractors established cost accounting practices.

(ii) Negotiate with the Contracting Officer to determine the terms and conditions under which a change may be made to a cost accounting practice, other than a change made under other provisions of paragraph (a)(4) of this clause; provided that no agreement may be made under this provision that will increase costs paid by the United States.

(iii) When the parties agree to a change to a cost accounting practice, other than a change under subdivision (a)(4)(i) of this clause, negotiate an equitable adjustment as provided in the Changes clause of this contract.

(5) Agree to an adjustment of the contract price or cost allowance, as appropriate, if the Contractor or a subcontractor fails to comply with an applicable Cost Accounting Standard, or to follow any cost accounting practice consistently and such failure results in any increased costs paid by the United States. Such adjustment shall provide for recovery of the increased costs to the United States, together with interest thereon computed at the annual rate established under section 6621(a)(2) of the Internal Revenue Code of 1986 (26 U.S.C. 6621(a)(2)) for such period, from the time the payment by the United States was made to the time the adjustment is affected. In no case shall the Government recover costs greater than the increased cost to the Government, in the aggregate, on the relevant contracts subject to the price adjustment, unless the Contractor made a change in its cost accounting practices of which it was aware or should have been aware at the time of price negotiations and which it failed to disclose to the Government.

(b) reserved
(c) The Contractor shall permit any authorized representatives of the Government to examine and make copies of any documents, papers, or records relating to compliance with the requirements of this clause.

(d) The Contractor shall include in all negotiated subcontracts which the Contractor enters into, the substance of this clause, except paragraph (b), and shall require such inclusion in all other subcontracts, of any tier, including the obligation to comply with all CAS in effect on the subcontractor's award date or if the subcontractor has submitted certified cost or pricing data, on the date of final agreement on price as shown on the subcontractors signed Certificate of Current Cost or Pricing Data. If the subcontract is awarded to a business unit which pursuant to 48 CFR 9903.201-2 is subject to other types of CAS coverage, the substance of the applicable clause set forth in subsection 30.201-4 of the Federal Acquisition Regulation shall be inserted. This requirement shall apply only to negotiated subcontracts in excess of $750,000, except that the requirement shall not apply to negotiated subcontracts otherwise exempt from the requirement to include a CAS clause as specified in 48 CFR 9903.201-1.

(End of clause)

I-212 52.230-3 DISCLOSURE AND CONSISTENCY OF COST ACCOUNTING PRACTICES OCT/2015

(a) The Contractor, in connection with this contract, shall--

(1) Comply with the requirements of 48 CFR 9904.401, Consistency in Estimating, Accumulating, and Reporting Costs; 48 CFR 9904.402, Consistency in Allocating Costs Incurred for the Same Purpose; 48 CFR 9904.405, Accounting for Unallowable Costs; and 48 CFR 9904.406, Cost Accounting Standard Cost Accounting Period, in effect on the date of award of this contract as indicated in 48 CFR Part 9904.

(2) (CAS-covered Contracts Only) If it is a business unit of a company required to submit a Disclosure Statement, disclose in writing its cost accounting practices as required by 48 CFR 9903.202-1 through 9903.202-5. If the Contractor has notified the Contracting Officer that the Disclosure Statement contains trade secrets and commercial or financial information which is privileged and confidential, the Disclosure Statement shall be protected and shall not be released outside of the Government.

(3)(i) Follow consistently the Contractors cost accounting practices. A change to such practices may be proposed, however, by either the Government or the Contractor, and the Contractor agrees to negotiate with the Contracting Officer the terms and conditions under which a change may be made. After the terms and conditions under which the change is to be made have been agreed to, the change must be applied prospectively to this contract, and the Disclosure Statement, if affected, must be amended accordingly.

(ii) The Contractor shall, when the parties agree to a change to a cost accounting practice and the Contracting Officer has made the finding required in 48 CFR 9903.201-6(c), that the change is desirable and not detrimental to the interests of the Government, negotiate an equitable adjustment as provided in the Changes clause of this contract. In the absence of the required finding, no agreement may be made under this contract clause that will increase costs paid by the United States.

(4) Agree to an adjustment of the contract price or cost allowance, as appropriate, if the Contractor or a subcontractor fails to comply with the applicable CAS or to follow any cost accounting practice, and such failure results in any increased costs paid by the United States. Such adjustment shall provide for recovery of the increased costs to the United States together with interest thereon computed at the annual rate established under section 6621(a)(2) of the Internal Revenue Code of 1986 (26 U.S.C. 6621(a)(2)), from the time the payment by the United States was made to the time the adjustment is affected.

(b) If the parties fail to agree whether the Contractor has complied with an applicable CAS, rule, or regulation as specified in 48 CFR 9903 and 9904 and as to any cost adjustment demanded by the United States, such failure to agree will constitute a dispute under 41 U.S.C. chapter 71, Contract Disputes.

(c) The Contractor shall permit any authorized representatives of the Government to examine and make copies of any documents, papers, and records relating to compliance with the requirements of this clause.

(d) The Contractor shall include in all negotiated subcontracts, which the Contractor enters into, the substance of this clause, except paragraph (b), and shall require such inclusion in all other subcontracts of any tier, except that—

(1) If the subcontract is awarded to a business unit which pursuant to 48 CFR 9903.201-2 is subject to other types of CAS coverage, the substance of the applicable clause set forth in subsection 30.201-4 of the Federal Acquisition Regulation shall be inserted.

(2) This requirement shall apply only to negotiated subcontracts in excess of $750,000.

(3) The requirement shall not apply to negotiated subcontracts otherwise exempt from the requirement to include a CAS clause as specified in 48 CFR 9903.201-1.

(End of clause)

I-217 252.225-7993 PROHIBITION ON PROVIDING FUNDS TO THE ENEMY (DEVIATION 2015-O0016) SEP/2015
(DEV 2015-O0016)

(a) The Contractor shall—

(1) Exercise due diligence to ensure that none of the funds, including supplies and services, received under this contract are provided directly or indirectly (including through subcontracts) to a person or entity who is actively opposing United States or Coalition forces involved in a contingency operation in which members of the Armed Forces are actively engaged in hostilities;

(2) Check the list of prohibited/restricted sources in the System for Award Management at www.sam.gov —

(i) Prior to subcontract award; and

(ii) At least on a monthly basis; and

(3) Terminate or void in whole or in part any subcontract with a person or entity listed in SAM as a prohibited or restricted source pursuant to subtitle E of Title VIII of the NDAA for FY 2015, unless the Contracting Officer provides to the Contractor written approval of the Head of the Contracting Activity to continue the subcontract.

(b) The Head of the Contracting Activity has the authority to—

(1) Terminate this contract for default, in whole or in part, if the Head of the Contracting Activity determines in writing that the contractor failed to exercise due diligence as required by paragraph (a) of this clause; or

(2)(i) Void this contract, in whole or in part, if the Head of the Contracting Activity determines in writing that any funds received under this contract have been provided directly or indirectly to a person or entity who is actively opposing United States or Coalition forces involved in a contingency operation in which members of the Armed Forces are actively engaged in hostilities.

(ii) When voided in whole or in part, a contract is unenforceable as contrary to public policy, either in its entirety or with regard to a segregable task or effort under the contract, respectively.

(c) The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts, including subcontracts for commercial items, under this contract that have an estimated value over $50,000 and will be performed outside the United States and its outlying areas.

(End of clause)

I-218 252.225-7995 CONTRACTOR PERSONNEL PERFORMING IN THE UNITED STATES CENTRAL COMMAND SEP/2017
(DEV 2015- AREA OF RESPONSIBILITY (DEVIATION 2017-O0004)
a) Definitions. As used in this clause—

"Combatant Commander" means the Commander of the United States Central Command Area of Responsibility.

"Contractors authorized to accompany the Force," or "CAAF," means contractor personnel, including all tiers of subcontractor

personnel, who are authorized to accompany U.S. Armed Forces in applicable operations and have been afforded CAAF status through a letter of authorization. CAAF generally include all U.S. citizen and third-country national employees not normally residing within the operational area whose area of performance is in the direct vicinity of U.S. Armed Forces and who routinely are collocated with the U.S. Armed Forces (especially in non-permissive environments). Personnel collocated with U.S. Armed Forces shall be afforded CAAF status through a letter of authorization. In some cases, Combatant Commander subordinate commanders may designate mission-essential host nation or local national contractor employees (e.g., interpreters) as CAAF. CAAF includes contractors previously identified as contractors deploying with the U.S. Armed Forces. CAAF status does not apply to contractor personnel in support of applicable operations within the boundaries and territories of the United States.

"Designated reception site" means the designated place for the reception, staging, integration, and onward movement of contractors deploying during a contingency. The designated reception site includes assigned joint reception centers and other Service or private reception sites.

"Law of war" means that part of international law that regulates the conduct of armed hostilities. The law of war encompasses all international law for the conduct of hostilities binding on the United States or its individual citizens, including treaties and international agreements to which the United States is a party, and applicable customary international law.

"Non-CAAF" means personnel who are not designated as CAAF, such as local national (LN) employees and non-LN employees who are permanent residents in the operational area or third-country nationals not routinely residing with U.S. Armed Forces (and third-country national expatriates who are permanent residents in the operational area) who perform support functions away from the close proximity of, and do not reside with, U.S. Armed Forces. Government-furnished support to non-CAAF is typically limited to force protection, emergency medical care, and basic human needs (e.g., bottled water, latrine facilities, security, and food when necessary) when performing their jobs in the direct vicinity of U.S. Armed Forces. Non-CAAF status does not apply to contractor personnel in support of applicable operations within the boundaries and territories of the United States.

"Subordinate joint force commander" means a sub-unified commander or joint task force commander.

(b) General.

(1) This clause applies to both CAAF and non-CAAF when performing in the United States Central Command (USCENTCOM) Area of Responsibility (AOR).

(2) Contract performance in USCENTCOM AOR may require work in dangerous or austere conditions. Except as otherwise provided in the contract, the Contractor accepts the risks associated with required contract performance in such operations.

(3) When authorized in accordance with paragraph (j) of this clause to carry arms for personal protection, contractor personnel are only authorized to use force for individual self-defense.

(4) Unless immune from host nation jurisdiction by virtue of an international agreement or international law, inappropriate use of force by contractor personnel authorized to accompany the U.S. Armed Forces can subject such personnel to United States or host nation prosecution and civil liability (see paragraphs (d) and (j)(3) of this clause).

(5) Service performed by contractor personnel subject to this clause is not active duty or service under 38 U.S.C. 106 note.

(c) Support.

(1)(i) The Combatant Commander will develop a security plan for protection of contractor personnel in locations where there is not sufficient or legitimate civil authority, when the Combatant Commander decides it is in the interests of the Government to provide security because—

(A) The Contractor cannot obtain effective security services;

(B) Effective security services are unavailable at a reasonable cost; or

(C) Threat conditions necessitate security through military means.

(ii) In appropriate cases, the Combatant Commander may provide security through military means, commensurate with the level of security provided DoD civilians.

(2)(i) Generally, CAAF will be afforded emergency medical and dental care if injured while supporting applicable operations. Additionally, non-CAAF employees who are injured while in the vicinity of U. S. Armed Forces will normally receive emergency medical and dental care. Emergency medical and dental care includes medical care situations in which life, limb, or eyesight is jeopardized. Examples of emergency medical and dental care include examination and initial treatment of victims of sexual assault; refills of prescriptions for life-dependent drugs; repair of broken bones, lacerations, infections; and traumatic injuries to the dentition. Hospitalization will be limited to stabilization and short-term medical treatment with an emphasis on return to duty or placement in the patient movement system.

(ii) When the Government provides emergency medical treatment or

transportation of Contractor personnel to a selected civilian facility, the Contractor

shall ensure that the Government is reimbursed for any costs associated with such treatment or transportation.

(iii) Medical or dental care beyond this standard is not authorized.

(3) Contractor personnel must have a Synchronized Predeployment and Operational Tracker (SPOT)-generated letter of authorization signed by the Contracting Officer in order to process through a deployment center or to travel to, from, or within the USCENTCOM AOR. The letter of authorization also will identify any additional authorizations, privileges, or Government support that Contractor personnel are entitled to under this contract. Contractor personnel who are issued a letter of authorization shall carry it with them at all times while deployed.

(4) Unless specified elsewhere in this contract, the Contractor is responsible for all other support required for its personnel engaged in the USCENTCOM AOR under this contract.

(d) Compliance with laws and regulations.

(1) The Contractor shall comply with, and shall ensure that its personnel performing in the USCENTCOM AOR are familiar with and comply with, all applicable—

(i) United States, host country, and third country national laws;

(ii) Provisions of the law of war, as well as any other applicable treaties and international agreements;

(iii) United States regulations, directives, instructions, policies, and procedures; and

(iv) Orders, directives, and instructions issued by the Combatant Commander, including those relating to force protection, security, health, safety, or relations and interaction with local nationals.

(2) The Contractor shall institute and implement an effective program to prevent violations of the law of war by its employees and subcontractors, including law of war training in accordance with paragraph (e)(1)(vii) of this clause.

(3) The Contractor shall ensure that CAAF and non-CAAF are aware—

(i) Of the DoD definition of "sexual assault" in DoDD 6495.01, Sexual Assault Prevention and Response Program;

(ii) That the offenses addressed by the definition are covered under the

Uniform Code of Military Justice (see paragraph (e)(2)(iv) of this clause). Other sexual

misconduct may constitute offenses under the Uniform Code of Military Justice, or another Federal law, such as the Military Extraterritorial Jurisdiction Act, or host nation laws; and

(iii) That the offenses not covered by the Uniform Code of Military Justice may nevertheless have consequences to the contractor employees (see paragraph (h)(1) of this clause).

(4) The Contractor shall report to the appropriate investigative authorities, identified in paragraph (d)(6) of this clause, any alleged offenses under—

(i) The Uniform Code of Military Justice (chapter 47 of title 10, United States Code) (applicable to contractors serving with or accompanying an armed force in the field during a declared war or contingency operations); or

(ii) The Military Extraterritorial Jurisdiction Act (chapter 212 of title 18, United States Code).

(5) The Contractor shall provide to all contractor personnel who will perform work on a contract in the deployed area, before beginning such work, information on the following:

(i) How and where to report an alleged crime described in paragraph (d)(4) of this clause.

(ii) Where to seek victim and witness protection and assistance available to contractor personnel in connection with an alleged offense described in paragraph (d)(4) of this clause.

(iii) This section does not create any rights or privileges that are not authorized by law or DoD policy.

(6) The appropriate investigative authorities to which suspected crimes shall be reported include the following—

(i) US Army Criminal Investigation Command at

http://www.cid.army.mil/index.html;

(ii) Air Force Office of Special Investigations at http://www.osi.af.mil;

(iii) Navy Criminal Investigative Service at http://www.ncis.navy.mil/Pages/publicdefault.aspx;

(iv) Defense Criminal Investigative Service at http://www.dodig.mil/HOTLINE/index.html;

(v) Any command of any supported military element or the command of any

base.

(7) Personnel seeking whistleblower protection from reprisals for reporting criminal acts shall seek guidance through the DoD Inspector General hotline at 800-424-9098 or www.dodig.mil/HOTLINE/index.html. Personnel seeking other forms of victim or witness protections should contact the nearest military law enforcement office.

(8) The Contractor shall ensure that Contractor employees supporting the U.S. Armed Forces deployed outside the United States are aware of their rights to—

(i) Hold their own identity or immigration documents, such as passport or driver's license;

(ii) Receive agreed upon wages on time;

(iii) Take lunch and work-breaks;

(iv) Elect to terminate employment at any time;

(v) Identify grievances without fear of reprisal;

(vi) Have a copy of their employment contract in a language they understand;

(vii) Receive wages that are not below the legal in-country minimum wage;

(viii) Be notified of their rights, wages, and prohibited activities prior to signing their employment contract; and

(ix) If housing is provided, live in housing that meets host-country housing and safety standards.

(e) Preliminary personnel requirements.

(1) The Contractor shall ensure that the following requirements are met prior to deploying CAAF (specific requirements for each category will be specified in the statement of work or elsewhere in the contract):

(i) All required security and background checks are complete and acceptable.

(ii) All CAAF deploying in support of an applicable operation—

(A) Are medically, dentally, and psychologically fit for deployment and performance of their contracted duties;

(B) Meet the minimum medical screening requirements, including theater-specific medical qualifications as established by the geographic Combatant Commander (as posted to the Geographic Combatant Commander's website or other venue); and

(C) Have received all required immunizations as specified in the contract.

(1) During predeployment processing, the Government will provide, at no cost to the Contractor, any military-specific immunizations and/or medications not available to the general public.

(2) All other immunizations shall be obtained prior to arrival at the deployment center.

(3) All CAAF and, as specified in the statement of work, select non-CAAF shall bring to the USCENTCOM AOR a copy of the U.S. Centers for Disease Control and Prevention (CDC) Form 731, International Certificate of Vaccination or Prophylaxis as approved by the World Health Organization, (also known as "shot record" or "Yellow Card") that shows vaccinations are current.

(iii) Deploying personnel have all necessary passports, visas, and other documents required to enter and exit the USCENTCOM AOR and have a Geneva Conventions identification card, or other appropriate DoD identity credential, from the deployment center.

(iv) Special area, country, and theater clearance is obtained for all personnel deploying. Clearance requirements are in DoD Directive 4500.54E, DoD Foreign Clearance Program. For this purpose, CAAF are considered non-DoD contractor personnel traveling under DoD sponsorship.

(v) All deploying personnel have received personal security training. At a minimum, the training shall—

(A) Cover safety and security issues facing employees overseas;

(B) Identify safety and security contingency planning activities; and

(C) Identify ways to utilize safety and security personnel and other resources appropriately.

(vi) All personnel have received isolated personnel training, if specified in the contract, in accordance with DoD Instruction 1300.23, Isolated Personnel Training for DoD Civilian and Contractors.

(vii) Personnel have received law of war training as follows:

(A) Basic training is required for all CAAF. The basic training will be provided through—

(1) A military-run training center; or

(2) A web-based source, if specified in the contract or approved by the Contracting Officer.

(B) Advanced training, commensurate with their duties and responsibilities, may be required for some Contractor personnel as specified in the contract.

(2) The Contractor shall notify all personnel who are not a host country national,

or who are not ordinarily resident in the host country, that such employees, and

dependents residing with such employees, who engage in conduct outside the United

States that would constitute an offense punishable by imprisonment for more than one year if the conduct had been engaged in within the special maritime and territorial jurisdiction of the United States, may potentially be subject to the criminal jurisdiction

of the United States in accordance with the Military Extraterritorial Jurisdiction Act of

2000 (18 U.S.C. 3261, et seq.);

(3) The Contractor shall notify all personnel that—

(i) Pursuant to the War Crimes Act (18 U.S.C. 2441), Federal criminal

jurisdiction also extends to conduct that is determined to constitute a war crime;

(ii) Other laws may provide for prosecution of U.S. nationals who commit offenses on the premises of U.S. diplomatic, consular, military or other U.S.

Government missions outside the United States (18 U.S.C. 7(9)) or non-U.S. nationals

who commit crimes against U.S. nationals in those places; and

(iii) In time of declared war or a contingency operation, CAAF are subject to the jurisdiction of the Uniform Code of Military Justice under 10 U.S.C. 802(a)(10).

(iv) Such employees are required to report offenses alleged to have been committed by or against contractor personnel to appropriate investigative authorities.

(v) Such employees will be provided victim and witness protection and assistance.

(f) Processing and departure points. CAAF shall—

(1) Process through the deployment center designated in the contract, or as otherwise directed by the Contracting Officer,

prior to deploying. The deployment center will conduct deployment processing to ensure visibility and accountability of contractor personnel and to ensure that all deployment requirements are met, including the requirements specified in paragraph (e)(1) of this clause;

(2) Use the point of departure and transportation mode directed by the Contracting Officer; and

(3) Process through a designated reception site (DRS) upon arrival at the deployed location. The DRS will validate personnel accountability, ensure that specific USCENTCOM AOR entrance requirements are met, and brief contractor personnel on theater-specific policies and procedures.

(g) Contractor Accountability and Personnel Data.

The Synchronized Predeployment and Operational Tracker (SPOT) is the joint web-based database to assist the Combatant Commanders in maintaining awareness of the nature, extent, and potential risks and capabilities associated with contracted support for contingency operations, humanitarian assistance and peacekeeping operations, or military exercises designated by USCENTCOM.

(1) Contractors shall account for all CAAF and non-CAAF personnel in SPOT by name.

(2) Registration. The Contractor shall comply with SPOT registration requirements.

(i) Contractor appointed company administrators for unclassified contracts shall register for a SPOT account at https://spot.dmdc.mil. For classified contracts, users shall access SPOT at https://spot.dmdc.osd.smil.mil.

(ii) Register in SPOT using one of the following log-in methods–

(A) A Common Access Card (CAC) or a SPOT-approved digital certificate; or

(B) A Government-sponsored SPOT user ID and password. This type of log-in method is only allowed for those individuals who are not authorized to obtain a CAC or an external digital certificate, and requires SPOT Program Management Office approval.

(iii) The SPOT Customer Support Team must validate user need. This process may take 2 business days. Contractor representatives will be contacted to validate contractor administrator account requests and determine the appropriate level of user access.

(iv) Refer to the OSD Program Support website at http://www.acq.osd.mil/log/PS/spot.html for the SPOT Business Rules, additional training resources, documentation regarding registration, and use of SPOT.

(3) Compliance with SPOT.

(i) The Contractor shall comply with the SPOT Business Rules located at http://www.acq.osd.mil/log/PS/spot.html.

(A) The Contractor shall enter into the SPOT web-based system the required information on Contractor personnel prior to deployment to the designated operational area and shall continue to use the SPOT web-based system to maintain accurate, up-to-date information throughout the deployment for applicable Contractor personnel.

(B) The Contractor shall ensure the in-theater arrival date (ITAD), deployment closeout dates and changes to the status of individual Contractor personnel relating to their ITAD and their duty location, to include closing out the deployment with

their proper status (e.g., mission complete, killed, wounded) are updated in the system in accordance with the processes and timelines established in the SPOT business rules.

(ii) SPOT non-compliance and deficiencies will be relevant to past performance evaluations for future contract opportunities in accordance with FAR subpart 42.15, Contractor Performance Information.

(h) Contractor personnel.

(1) The Contracting Officer may direct the Contractor, at its own expense, to remove and replace any contractor personnel who jeopardize or interfere with mission accomplishment or who fail to comply with or violate applicable requirements of this contract. Such action may be taken at the Government's discretion without prejudice to its rights under any other provision of this contract, including the Termination for Default clause.

(2) The Contractor shall identify all personnel who occupy a position designated as mission essential and ensure the continuity of essential Contractor services during designated operations, unless, after consultation with the Contracting Officer, Contracting Officer's representative, or local commander, the Contracting Officer directs withdrawal due to security conditions.

(3) The Contractor shall ensure that contractor personnel follow the guidance at paragraph (e)(2)(v) of this clause and any specific Combatant Commander guidance on reporting offenses alleged to have been committed by or against contractor personnel to appropriate investigative authorities.

(4) Contractor personnel shall return all U.S. Government-issued identification, to include the Common Access Card, to appropriate U.S. Government authorities at the end of their deployment (or, for non-CAAF, at the end of their employment under this contract).

(i) Military clothing and protective equipment.

(1) Contractor personnel are prohibited from wearing military clothing unless specifically authorized in writing by the Combatant Commander. If authorized to wear military clothing, contractor personnel must—

(i) Wear distinctive patches, arm bands, nametags, or headgear, in order to be distinguishable from military personnel, consistent with force protection measures; and

(ii) Carry the written authorization with them at all times.

(2) Contractor personnel may wear military-unique organizational clothing and individual equipment (OCIE) required for safety and security, such as ballistic, nuclear, biological, or chemical protective equipment.

(3) The deployment center, or the Combatant Commander, shall issue OCIE and shall provide training, if necessary, to ensure the safety and security of contractor personnel.

(4) The Contractor shall ensure that all issued OCIE is returned to the point of issue, unless otherwise directed by the Contracting Officer.

(j) Weapons.

(1) If the Contractor requests that its personnel performing in the USCENTCOM AOR be authorized to carry weapons for individual self-defense, the request shall be made through the Contracting Officer to the Combatant Commander, in accordance with DoD Instruction 3020.41. The Combatant Commander will determine whether to authorize in-theater contractor personnel to carry weapons and what weapons and ammunition will be allowed.

(2) If contractor personnel are authorized to carry weapons in accordance with paragraph (j)(1) of this clause, the Contracting

Officer will notify the Contractor what weapons and ammunition are authorized.

(3) The Contractor shall ensure that its personnel who are authorized to carry weapons—

(i) Are adequately trained to carry and use them—

(A) Safely;

(B) With full understanding of, and adherence to, the rules of the use of force issued by the Combatant Commander; and

(C) In compliance with applicable agency policies, agreements, rules, regulations, and other applicable law;

(ii) Are not barred from possession of a firearm by 18 U.S.C. 922;

(iii) Adhere to all guidance and orders issued by the Combatant Commander regarding possession, use, safety, and accountability of weapons and ammunition;

(iv) Comply with applicable Combatant Commander and local commander force-protection policies; and

(v) Understand that the inappropriate use of force could subject them to U.S. or host-nation prosecution and civil liability.

(4) Whether or not weapons are Government-furnished, all liability for the use of any weapon by contractor personnel rests solely with the Contractor and the Contractor employee using such weapon.

(5) Upon redeployment or revocation by the Combatant Commander of the Contractor's authorization to issue firearms, the Contractor shall ensure that all Government-issued weapons and unexpended ammunition are returned as directed by the Contracting Officer.

(k) Vehicle or equipment licenses. Contractor personnel shall possess the required licenses to operate all vehicles or equipment necessary to perform the contract in the USCENTCOM AOR.

(l) Purchase of scarce goods and services. If the Combatant Commander has established an organization for the USCENTCOM AOR whose function is to determine that certain items are scarce goods or services, the Contractor shall coordinate with that organization local purchases of goods and services designated as scarce, in accordance with instructions provided by the Contracting Officer.

(m) Evacuation.

(1) If the Combatant Commander orders a mandatory evacuation of some or all personnel, the Government will provide assistance, to the extent available, to United States and third country national contractor personnel.

(2) In the event of a non-mandatory evacuation order, unless authorized in writing by the Contracting Officer, the Contractor shall maintain personnel on location sufficient to meet obligations under this contract.

(n) Next of kin notification and personnel recovery.

(1) The Contractor shall be responsible for notification of the employee-designated next of kin in the event an employee dies, requires evacuation due to an injury, or is isolated, missing, detained, captured, or abducted.

(2) The Government will assist in personnel recovery actions in accordance with

DoD Directive 3002.01E, Personnel Recovery in the Department of Defense.

(o) Mortuary affairs. Contractor personnel who die while in support of the U.S. Armed Forces shall be covered by the DoD mortuary affairs program as described in DoD Directive 1300.22, Mortuary Affairs Policy, and DoD Instruction 3020.41, Operational Contractor Support.

(p) Changes. In addition to the changes otherwise authorized by the Changes clause of this contract, the Contracting Officer may, at any time, by written order identified as a change order, make changes in the place of performance or Government-furnished facilities, equipment, material, services, or site. Any change order issued in accordance with this paragraph (p) shall be subject to the provisions of the Changes clause of this contract.

(q) Subcontracts. The Contractor shall incorporate the substance of this clause, including this paragraph (q), in all subcontracts when subcontractor personnel are performing in the USCENTCOM AOR.

(End of clause)

I-219 252.225-7997 CONTRACTOR DEMOBILIZATION (DEVIATION 2013-O0017) AUG/2013
(DEV 2013-O0017)

(a) Generally, the Contractor is responsible for demobilizing all of its personnel and equipment from the Afghanistan Combined Joint Operations Area (CJOA).

(b) Demobilization plan. The Contractor shall submit a demobilization plan to the Contracting Officer for approval a minimum of 120 calendar days prior to the end of the current contract performance period or as otherwise directed by the Contracting Officer. Upon acceptance of the demobilization plan by the Contracting Officer, the demobilization plan becomes a material part of the contract and the Contractor agrees to fully perform its demobilization in accordance with that plan. The demobilization plan shall address the items specified in this clause and must demonstrate the Contractors plans and ability to remove its personnel and equipment from the CJOA and to return Government property no later than 30 days after the expiration of the current period of performance.

(c) Demobilization plan implementation. Every 30 calendar days after incorporation of the plan into the contract, or as otherwise directed by the Contracting Officer, the Contractor shall provide written information to the Contracting Officer and Contracting Officer Representative that addresses the Contractors progress in implementing the plan. The Contractor shall continue to provide the information in the preceding sentence until the Contractor has completely and properly demobilized. If the Contracting Officer or Contracting Officer Representative identifies deficiencies with the plan, as approved, or with the implementation of that plan, the Contractor shall submit a corrective action plan (CAP) to those officials within five calendar days to remedy those deficiencies. The Contracting Officer shall review the CAP within five calendar days to determine whether the CAP is acceptable. Upon approval by the Contracting Officer, the CAP becomes a material part of the demobilization plan.

(d) Plan contents

(1) The plan shall identify the method of transportation (air, ground) the Contractor intends to use to remove its personnel and equipment from the CJOA and whether that method of transportation is Government or Contractor-furnished. If Government-furnished transportation is authorized, the plan must identify the contract term or condition which authorizes Government transportation of the personnel and equipment associated with this contract.

(2) The plan shall identify the number of Contractor personnel to be demobilized by category (U.S. citizens, Third Country Nationals (TCN), Local Nationals (LN)) and, for U.S. and TCN personnel, identify the point of origin or home country to which they will be transported and the timeline for accomplishing that objective. If U.S. or TCN employees have authorization to remain in the CJOA after completion of demobilization, the plan shall identify the name each individual, their nationality, their location in the CJOA, and provide a copy of the authorization. The plan shall also identify whether the Contractor needs the Contracting Officer to extend the Letters of Authorization (LOA) for any Contractor personnel to execute the demobilization plan.

(3) The plan shall identify all Contractor equipment and the timeline for accomplishing its demobilization. The Contractor shall identify all equipment, whether or not it is covered by CJTSCC Acquisition Instruction Clause Inbound / Outbound Cargo and Contractor Equipment Census. The plan shall also specify whether the Contractor intends to leave any equipment in the CJOA, a list of all such equipment, including its location, and the reason(s) therefor.

(4) The plan shall identify all Government property provided or made available to the Contractor under this contract or through any separate agreement or arrangement (e.g., Installation Mayors, Garrison Commanders). The plan shall also identify the timeline for vacating or returning that property to the Government, including proposed dates for conducting joint inspections.

(e) Demobilization requirements:

(1) The Contractor shall demobilize and return its personnel to their point of origin or home country according to the approved demobilization plan.

(2) The Contractor is not authorized to use Government-furnished transportation unless specifically authorized in this contract.

(3) The Contractor may request an extension of the LOAs only for those Contractor personnel whose presence is required to execute the approved demobilization plan. The Contractor shall submit its request no later than 30 calendar days prior to the expiration of the current period of performance. LOAs may only be extended for a period up to 30 calendar days after expiration of the current performance period. The request shall contain the following information:

(i) The names of each individual requiring an extension.

(ii) The required extension period.

(iii) The justification for each extension (e.g., the specific function(s) the individual will perform during the demobilization period). The Contractor is not entitled to any additional compensation if LOAs are extended.

(4) The Contractor shall close out their employee's deployments with the proper status entered into the Synchronized Pre-Deployment Operational Tracker (SPOT) database (e.g. active, redeployed, no-shows, killed, injured) within 72 hours of their employee's redeployment and, if applicable, release their personnel in SPOT.

(5) All Contractor equipment that is lost, abandoned or unclaimed personal property that comes into the custody or control of the Government after the demobilization period has ended may be sold or otherwise disposed of in accordance with 10 U.S.C. section 2575. Notwithstanding the previous sentence and the Governments authority under 10 U.S.C. section 2575, the Government may exercise any other contractual rights for the Contractors failure to perform in accordance with its demobilization plan.

(6) If the Contractor waives its interest to all lost, abandoned or unclaimed personal property, the Contractor may still be liable for all costs incurred by the Government to remove or dispose of the abandoned property.

(7) The Government may dispose of any and all lost, unclaimed, or abandoned personal property in accordance with 10 U.S.C. section 2575.

(8) The Contractor shall return all Government property provided or made available under this contract or through any separate agreement. The Contractor shall report all lost or damaged Government property in accordance with DFARS 52.245-1(h) unless other procedures are identified in the contract or separate agreement. If the Government inspects the property and finds that damages or deficiencies have not been reported by the end of the demobilization period, the Government may reduce payments under the contract by the amounts required to correct the damages or deficiencies or replace the loss.

(9) The Contractor is liable for all cleanup, clearing, and/or environmental remediation expenses incurred by the Government in returning a Government facility to its original condition. If damages or deficiencies are discovered during the inspection of said facility, the Contractor shall make the necessary repairs or corrections and then notify the Installation Mayor, Garrison Commander, or their designees to arrange for a re-inspection of the facility. If the Installation Mayor or Garrison Commander inspects the facility and finds that damages or deficiencies have not been repaired or corrected by the end of the demobilization period, the Government may reduce payments under the contract by the amounts required to correct the damages or deficiencies.

(10) The Contractor shall ensure that all employees, including all subcontractor employees at all tiers, return installation and/or access badges to the local Access Control Badging Office for de-activation and destruction according to the approved demobilization plan. The Contractor shall submit a Badge Termination Report to ensure each record is flagged and the badge is revoked. If an

employees badge is not returned, the Contractor shall submit a Lost, Stolen or Unrecovered Badge Report to the appropriate Access Control Badging Office. Contractor employees in possession of a Common Access Card (CAC) shall be responsible for turning in the CAC upon re-deployment through a CONUS Replacement Center in the United States. Failure to comply with these requirements may result in delay of final payment.

(f) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (f), in all subcontracts.

(End of Clause)

K-1 52.204-24 REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO AUG/2019
SURVEILLANCE SERVICES OR EQUIPMENT

(a) Definitions. As used in this provision--
"Covered telecommunications equipment or services", "Critical Technology", and "Substantial or essential component" have the meanings provided in clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Prohibition. 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. Contractors are not prohibited 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.

(c) Representation. The Offeror represents that--
It [ ] will, [ ] will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation.
(d) Disclosures. If the Offeror has responded affirmatively to the representation in paragraph (c) of this provision, the Offeror shall provide the following information as part of the offer--

(1) All covered telecommunications equipment and services offered (include brand; model number, such as original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);
(2) Explanation of the proposed use of covered telecommunications equipment and services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b) of this provision;
(3) For services, the entity providing the covered telecommunications services (include entity name, unique entity identifier, and Commercial and Government Entity (CAGE) code, if known); and
(4) For equipment, the entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known).

(End of provision)

APPENDIX 4: REFERENCE PUBLICATIONS

APPLICABLE PUBLICATIONS
The contractor must abide by all applicable regulations, publications, manuals, Security Technical Implementation Guides (STIGs) and local policies and procedures.

The following specifications, standards, policies and procedures represent the constraints placed on this acquisition. All documents listed are mandatory, as applicable. Applicability is as defined in the document. The most current version of the document at the time of task order issuance will take precedence. The list is not all-inclusive. **Other documents required for execution of tasks issued under ITES-3S will be cited in the relevant task order.**

1. Army Enterprise Standardization

1.1 The Department of Defense Strategy for Implementing the Joint Information Environment, 18 September 2013, http://dodcio.defense.gov/Portals/0/Documents/JIE/2013-09-13_DoD_Strategy_for_Implmenting_JIE_(NDAA_931)_Final_Document.pdf

1.2 U.S. Army Network Operations Reference Architecture (Aligned to the DOD Enterprise) Version 1.0, 6 March 2014, http://ciog6.army.mil/Portals/1/Architecture/2014/20140306-US_Army_NetOps_Reference_Architecture_and_Annex_A-V1-0.pdf

1.3 U.S. Army Unified Capabilities Reference Architecture Version 1.0, 11 October 2013, http://ciog6.army.mil/Portals/1/Architecture/Army%20UC%20RA%20%20v1.0--03%20October13%20reduced%20size%2019%20Nov%202013.pdf

1.4 U.S. Army – Identity and Access Management Reference Architecture (Aligned to the DOD Enterprise) Version 4.0, 29 September 2014, http://ciog6.army.mil/Portals/1/Architecture/2014/20140929-US_Army_Identity_and_Access_Management_Reference_Architecture_V4-0.pdf

1.5 U.S. Army Network Security Reference Architecture (Aligned to the DOD Enterprise) Version 2.0, 29 September 2014, http://ciog6.army.mil/Portals/1/Architecture/2014/20140929-US_Army_Network_Security_Reference_Architecture_V2-0.pdf

1.6 U.S. Army Thin/Zero Client Computing Reference Architecture Version 1.0, 14 March 2013, http://ciog6.army.mil/Portals/1/Architecture/ApprovedThinClient-ZeroComputingReferenceArchitecturev1-0_14Mar13.pdf

1.7 Under Secretary of the Army Memorandum, Migration of Army Enterprise Systems/Applications to the Core Data Centers, 9 June 2014, http://ciog6.army.mil/Portals/1/Policy/2014/USA_Policy_Memo_Application%20Migration%20to_Core_Data_Centers_Jun_9_2014.pdf

1.8 Office of the Secretary of the Army Memorandum, Army Mobility Strategy, 21 November 2013, http://ciog6.army.mil/Portals/1/Policy/2013/Army%20Mobility%20Strategy_26NOV2013.pdf

1.9 Army Enterprise Desktop Software Standardization (TECHCON 2003-005c), 13 September 2006. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736239

1.10 ASA-ALT Memorandum, Enterprise Software Agreements, 29 December 2006, https://chess.army.mil/Content/files/%287034%29ESA_Memo.pdf

1.11 DFARS Final Rule on the use of Enterprise Software Agreements. 25 October 2002, https://chess.army.mil/Content/files/DFARS_ESI_Final_Rule.pdf

1.12 Acquiring Commercially Available Software and Information Technology (IT) Products within the Army. AR 25-1, 25 June 2013, paragraph 2-16 h. http://www.apd.army.mil/pdffiles/r25_1.pdf

1.13 Use of Computer Hardware, Enterprise Software and Solutions (CHESS) as the Primary Source for Procuring Commercial Information technology (IT) Hardware and Software, 4 May 2009 https://chess.army.mil/Content/files/Use_of_CHESS_memo.pdf

1.14 Use of Defense Switched Network in lieu of Federal Telecommunications Service / Public Switched Telephone Network (Implementation Memorandum 2005-12), 27 January 2006 https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736291

1.15 Electromagnetic Capability Guidance for Installation of Personal Communication Service (PCS) System Antenna Towers on Army Installations (Implementation Memorandum 2005-06), 3 January 2006, https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736288

1.16 Information Management Policy, Internet Protocol (IP) Space Management, Network Address Translation (Implementation Memorandum 2004-19), 15 December 2004. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736287

1.17 Support for Army Morale, Welfare, Recreation, and Lodging, and Family Program Information Systems on Army Installations (Implementation Memorandum 2004-17), 28 December 2004. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736286

1.18 Enterprise Telephony Firewall Management System (Implementation Memorandum 2004-14), 28 February 2005. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736278

1.19 Email Attachment Filtering (TECHCON 2004-011A) 6 May 2006. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736275

1.20 Command, Control, Computers and Communication Information Technology (C4/IT) Support for Army Reserve Tenants on Army Installations (TECHCON 2004-010), 15 September 2004. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736264

1.21 Defense Research and Engineering Network Implementation of Army Installations (TECHCON 2004-009A) 6 May 2006. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736263

1.22 Active Directory Management Roles and Responsibilities (TECHCON 2004-008), 29 March 2005. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736262

1.23 Guidance for Terminating Dedicated WAN and Virtual Ethernet Circuits from CONUS Army Posts, Camps, and Stations to Off-Post Enclaves (TECHCON 2004-007), 2 Feb 2005 https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736261

1.24 Networthiness Certification for Tactical Systems (TECHCON 2004-005), 19 August 2004. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736260

1.25 Army Enterprise Active Directory Windows Internet Name Service Configuration (TECHCON 2004-004), 15 October 2004. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736257

1.26 Army Enterprise Active Directory Site-Level Domain Controller Installation Guidelines (TECHCON 2004-001B), February 11, 2005. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736255

1.27 Fielding Non-Army Systems on Army Installations (TECHCON 2003-002), 28 May 2003. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736253

1.28 Implementation of Deployable Forces Forests within the General Force Infrastructure in the Army Enterprise Infrastructure Active Directory Environment (TA 2006-006), 14 May 2007. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=7780784

1.29 Operation and Management of PM-Managed Systems in the Army Enterprise Infostructure Active Directory Environment (TA 2005-018) 14 September 2006. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736242

1.30 Common Access Card Cryptographic Logon Implementation (TA 2005-009), 1 March 2006. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=7107237

1.31 Electromagnetic Compatibility Guidance for Installation of Personal Communication Service System Antenna Towers on Army Installations (TA 2005-006) 3 January 2006. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=7231353

1.32 Remote Access Virtual Private Network Implementation on Army Installations (TA 2005-004), 8 June 2006. https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736241

1.33 Request, Approval, and Implementation of Active Directory Trusts within the Army Enterprise Infostructure (TA 2004-015a), 7 February 2006, https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=7405333

1.34 Technical Guidance MWR for Non-Franchised Users, 4 February 2003, https://www.us.army.mil/suite/collaboration/GetDocument.do?doid=6736222

1.35 Army Thin Client Computing Guidance, SAIS-AOI, November 15, 2010, http://ciog6.army.mil/Portals/1/Policy/2012/Army%20Thin%20Client%20Guidance_15NOV2010.pdf

1.36 Technical Authority (TA) Implementation Memorandum For Army End-User Computing Environment, Version 3, 16 October 2015 (NETC-OP-E-AGM-15-1132-v3 NETCOM

2. Army Knowledge Management

2.1 DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009, http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf

2.2 Army Knowledge Management Implementation Plan(Version 2.0), 01 September 2003, https://www.us.army.mil/suite/doc/6155268 (requires AKO login)

3. Active Directory

3.1 The Army Enterprise Network Operations (NetOps) Integrated Architecture (AENIA) Requirements Document (ARD) For Active Directory Services Management. 15 August 2007, (requires AKO Login). https://www.us.army.mil/suite/doc/13985332
3.2 Request, Approval, and Implementation of Active Directory Trusts within the Army Enterprise Infostructure (AEI) – TECHCON 2004-015A. 7 February 2006, (Requires AKO Login) https://www.us.army.mil/suite/doc/7405333

3.3 Active Directory Management Roles and Responsibilities – TECHCON 2004-008, 29 March 2005, https://www.us.army.mil/suite/doc/6736262

4. Networthiness Program
4.1 DoD CIO Memorandum, Interim Guidance on Networthiness of Information Technology (IT) Connected to DoD Networks, 22 November 2011, http://www.disa.mil/Services/Network-Services/~/media/Files/DISA/Services/UCCO/DoD_Networthiness_Memorandum.pdf

4.2 Networthiness Certification Program, (Requires CAC Login)
https://west.esps.disa.mil/netcom/sites/nw/CoNApproval/Lists/Networthiness%20Data/NWPublicView.aspx

5. DoD Information Technology Standards Registry
5.1 DOD Information Technology Standards Registry (Note: Access to the DISR requires registration/login to the GIG Technical Guidance Federation website) https://gtg.csd.disa.mil (Requires CAC Login)

6. Information Assurance – Army and DOD Policy
6.1 Information Assurance (AR 25-2), http://www.apd.army.mil/pdffiles/r25_2.pdf

6.2 Information Assurance Best Business Practice, Information Assurance Tools (version 2.0), 1 August 2014, https://www.milsuite.mil/book/servlet/JiveServlet/download/22811-24-509312/03-DC-O-

6.3 DOD Instruction 8510.01, 12 March 2014, Risk Management Framework (RMF) for DoD Information Technology (IT), http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

6.4 Disposition of Unclassified DOD Computer Hard Drives**.** *4 June 2001*, Effective 4 June 2001, http://www.au.af.mil/au/holmcenter/AFJROTC/documents/DispositionofUnclassifiedDoDComputerHardDrives.pdf

6.5 DODI 8330.01, Interoperability of Information Technology (IT), Including National Security Systems (NSS), May 21, 2014. http://www.dtic.mil/whs/directives/corres/pdf/833001p.pdf

6.6 CJCSI 6212.01F Net Ready Key Performance Parameter (NR KPP), 21 March 2012, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf

6.7 DOD Instruction 5200.01, "DOD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008, http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf

6.8 DOD Instruction O-8530.2, Support to Computer Network Defense (CND), March 9, 2001, (Requires DoD Common Access Card (CAC) for access) https://whsddpubs.dtic.mil/corres/pdf/O85302p.pdf

6.9 DOD Instruction 8500.01, Cybersecurity, 14 March 2014, http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

6.10 DODI 8580.1, Information Assurance (IA) in the Defense Acquisition System, 9 June 2004, http://www.dtic.mil/whs/directives/corres/pdf/858001p.pdf

6.11 DODD 8570.01, Information Assurance Training, Certification, and Workforce Management, 23 April 2007, http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf

6.12 DEPARTMENT OF DEFENSE (DOD) 8570.01-M, CHANGE 3, INFORMATION ASSURANCE WORKFORCE IMPROVEMENT PROGRAM, 24 January 2012. http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

6.13 CIO/G6, CYBER DIRECTORATE, BEST BUSINESS PRACTICE 05-PR-M-0002, IA TRAINING AND CERTIFICATION, VERSION 5.0, 06 March 2012 https://ia.signal.army.mil/docs/pub.trainingandcertificationbbpfinal10.pdf

6.14 Defense Acquisition Guidebook _ Chapter 7 Acquiring Information Technology and National Security Systems, Section 7.5 Information Assurance https://dag.dau.mil/Pages/Default.aspx

6.15 DOD CIO Memorandum, Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media, 3 July 2007; URL- http://www.dod.gov/pubs/foi/privacy/docs/dod_dar_tpm_decree07_03_071.pdf

6.16 ALARACT 284/2011 - COMPUTING ENVIRONMENT (CE) CERTIFICATIONS FOR THE ARMY INFORMATION ASSURANCE (IA) WORKFORCE, https://www.us.army.mil/suite/doc/31460103

7. Information Assurance – NIST Policy and Guidelines
7.1 National Security Telecommunications and Information Systems Security (NSTISSP) Policy No. 11, July 2003 http://www.niap-ccevs.org/cc-scheme/nstissp_11_revised_factsheet.pdf

7.2 Guide to Information Technology Security Services NIST Special Publication 800-35**.** *October 2003,* http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf

7.3 Guide to Selecting Information Technology Security Products NIST Special Publication 800-36. October 2003, http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

7.4 Guide for Applying the Risk Management Framework to Federal Information Systems Special Publication 800-37. Feb 2010, http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

7.5 Guide to General Server Security, Special Publication 800-123, July 2008, http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

7.6 Common Criteria http://www.commoncriteriaportal.org/

7.7 Security and Privacy Controls for Federal Information Systems and Organizations SP 800-53 Rev. 4, 30 April 2013; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

8. Information Management
8.1 Department of Defense Global Information Grid Architecture Architectural Vision, June 2007, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484389

8.2 Army Information Architecture Version 4.1, 5 June 2013, http://ciog6.army.mil/Portals/1/Architecture/ArmyInformationArchitecturev4-1dtd2013-06-05.pdf

8.3 DoD Information Enterprise Architecture (Version 2.0), July 2012 http://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD%20IEA%20v2.0_Volume%20I_Description%20Document_Final_20120730.pdf

8.4 DoD Instruction 8320.02, "Data Sharing in a Net-Centric Department of Defense. 02 December 2004, http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf

8.5 The Department of Defense Architecture Framework (DoDAF) version 2.02. March 2011, http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf

8.6 DoD CIO Desk Reference - The Clinger-Cohen Act (Chapter 25 of title 40, United States Code) see http://dodcio.defense.gov/Portals/0/Documents/ciodesrefvolone.pdf

8.7 OMB Circular A-130 Revised, "Management of Federal Information Resources, Transmittal 4, 28 November 2000 http://www.whitehouse.gov/omb/circulars_a130_a130trans4

8.8 CJCSI 3170.01I: Joint Capabilities Integration and Development System, 23 January 2015, https://dap.dau.mil/policy/Documents/2015/CJCSI_3170_01I.pdf

8.9 Department of Defense Net-Centric Data Strategy, 9 May 2003. http://dodcio.defense.gov/Portals/0/Documents/DIEA/Net-Centric-Data-Strategy-2003-05-092.pdf

8.10 OASD(NII), Net-Centric Checklist, Version 2.1.3, May 2004, http://dodcio.defense.gov/Portals/0/Documents/NetCentric_Checklist_v2-1-3_.pdf

8.11 Joint Net-Centric Operations (JNO) Capability Portfolio Management (CPM), Business Plan Version 1.0. April 16, 2007, https://acc.dau.mil/adl/en-US/257395/file/40330/JNO%20Business%20Plan%20Version%201%20April%202007%20(2).pdf

9. Unified Capabilities and IPv6
9.1 Internet Protocol version 6 (IPv6) for the GSCR, http://jitc.fhu.disa.mil/tssi/docs/1_7ipv6_approved6089r6104.pdf

9.2 Unified Capabilities Approved Product List Process, http://www.disa.mil/Services/Network-Services/UCCO?panel=1

9.3 Unified Capabilities Approved Product List – DISA https://aplits.disa.mil/processAPList.action

9.4 DoD CIO Memorandum, DoD Internet Protocol Version 6 (IPv6) Definitions, 26 June 2008, http://www.hpc.mil/images/hpcdocs/ipv6/signed-dod-ipv6-definitions-memo-bw-rev.pdf

9.5 OMB Memorandum M-05-22, Transition Planning for Internet Protocol Version 6 (IPv6), 2 August 2005, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-22.pdf

9.6 DoD CIO Memorandum, DoD Internet Protocol Version 6 (IPv6) Interim Transition Guidance, 29 September 2003, http://www.hpc.mil/images/hpcdocs/ipv6/dod_cio_september_23_policy_ltr.pdf

9.7 DoD CIO Memorandum, DoD Internet Protocol Version 6 (IPv6), 9 June 2003, http://www.defense.gov/news/Jun2003/d20030609nii.pdf

9.8 Federal Register / Vol. 74, No. 236 / Thursday, December 10, 2009 / Rules and Regulations, http://www.gpo.gov/fdsys/pkg/FR-2009-12-10/pdf/E9-28928.pdf

10. Smart Cards

10.1 Army CAC/PKI Program Card Reader Specifications, Rev. 7 March 2007, https://chess.army.mil/Content/files/2007_03_07_the_smart_card_update.pdf

10.2 Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS Pub 201-2, August 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

10.3 Access Card Office (ACO); Common Access Card (CAC) Release 1.0 Reader Specifications, Version 1.0 (September 25, 2000)**,** http://www.dmdc.osd.mil/smartcard/images/CACRelease1ReaderSpecificationv1Specification.pdf

10.4 Government Smart Card Interoperability Specification**.** *Version 2.1 – 16 July 2003*, http://csrc.nist.gov/publications/nistir/nistir-6887.pdf

11. Radio Frequency Identification (RFID)

11.1 DOD 4140.1-R DOD Supply Chain Materiel Management Regulation, May 23, 2003 http://www.acq.osd.mil/log/sci/exec_info/drid/p41401r.pdf

11.2 Department of Defense Standard Practice - Military Marking For Shipment and Storage (MIL-STD-129P w/CHANGE 4) 19 September 2007, http://www.acq.osd.mil/log/sci/ait/mil-std-129pch4.pdf

11.3 RF-Tag Format (Version 2.0). 10 May 2002, http://www.ndia.org/Divisions/Divisions/Logistics/Documents/Content/ContentGroups/Divisions1/Logistics/4RF_Tag_Data_Specification_V2.pdf

11.4 Policy for Unique Identification (UID) of Tangible Items – New Equipment, Major Modifications, and Reprocurements of Equipment and Spares. 29 July 2003, http://www.acq.osd.mil/dpap/UID/uid_signed_policy_memo_2003.07.29.pdf

11.5 Update to Policy For Unique Identification (UID) of Tangible Items – New Equipment, Major Modifications, and Reprocurements of Equipment and Spare. 3 Sep 2004, http://www.acq.osd.mil/dpap/Docs/uid/Sep.%203%20UID%20%20Policy%20Update.pdf

11.6 Policy For Unique Identification (UID) of Tangible Personnel Property Legacy Items in Inventory and Operational Use, Including Government Furnished Property (GFP). 23 Dec 2004, http://www.acq.osd.mil/dpap/Docs/uid/UID%20Policy%20Update%20Legacy%20Items%2012-23-2004.pdf

11.7 Department of Defense Guide to Uniquely Identifying Items (Version 1.4). 16 April 2004, http://www.acq.osd.mil/dpap/Docs/uid/guide_1_4.pdf

11.8 Department of Defense Standard Practice – Identification Marking of US Military Property (MIL-STD-130L). 20 Dec 2004, http://www.acq.osd.mil/dpap/Docs/uid/MIL-STD-130L%20Change1.pdf

11.9 Unique Identification 101 – The Basics. November 2004, http://www.acq.osd.mil/dpap/Docs/uid/UID 101.pdf

11.10 Passive RFID DFARS Clause 252.211-7006, http://www.acq.osd.mil/dpap/dars/dfars/html/current/252211.htm#252.211-7006

11.11 DOD Supplier's Passive RFID Information Guide, Version 15.0, http://www.acq.osd.mil/log/sci/ait/DoD_Suppliers_Passive_RFID_Info_Guide_v15update.pdf

11.12 Radio Frequency Identification (RFID) Policy, 30 July 2004, https://acc.dau.mil/adl/en-US/142796/file/27748/RFIDPolicy07-30-2004.pdf

12. Logistics
12.1 DoD 4140.1-R DoD Supply Chain Materiel Management Regulation, May 23, 2003 http://www.acq.osd.mil/log/sci/exec_info/drid/p41401r.pdf

12.2 Deputy Under Secretary of Defense (Logistics and Materiel Readiness) Logistics Enterprise Integration and Transformation, November 2001 http://www.acq.osd.mil/log/logistics_materiel_readiness/organizations/lsm/assetts/feb_02_information/ei_info/Ent%20Integ%20and%20Transformation%20Dec%2001.doc

13. Voice Over IP (VOIP)
13.1 Security Considerations for Voice Over IP Systems, Special Publication 800-58. January 2005, http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf

13.2 DISA Memo, Voice Video over Internet Protocol (VVoIP) STIG, Ver 3, Rel7 23 Oct 2015, http://iase.disa.mil/stigs/pages/a-z.aspx (search name and download files)

14. Wireless
14.1 Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG) (DoD Directive 8100.2). Certified current as of 23 Apr 2007, http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf

14.2 Security Requirements for Cryptographic Modules (FIPS PUB 140-2). 25 May 2001, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

14.3 FIPS 140-1 and FIPS 140-2 Cryptographic Modules Validation List. March 10, 2009, http://csrc.nist.gov/groups/STM/cmvp/

14.4 DISA Wireless STIG, Version 6 Rel 9, 24 Oct 2014 http://iase.disa.mil/stigs/pages/a-z.aspx (search on name and download files)

14.5 Information Assurance Best Business Practice, Wireless Security Standards, Version 4 (09-EC-M-0010), 26 June 2013, https://bop.peostri.army.mil/sites/bop/Lists/Request%20for%20Proposals/Attachments/67/Attachment%209%20-%20DA%2009-EC-M-0010%20IA%20Best%20Business%20Practice%20on%20Wireless%20Security%20Standards%2003282014.pdf

15. Section 508
15.1 Section 508. http://www.section508.gov

15.2 Workforce Investment Act of 1998, Section 508 – Electronic and Information Technology. 21 December 2000, http://www.usdoj.gov/crt/508/508law.pdf

15.3 Guide to the Section 508 Standards for Electronic and Information Technology: Software Applications and Operating Systems (1194.21) http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/guide-to-the-section-508-standards/software-applications-and-operating-systems-1194-21 , Web-based Intranet and Internet Information and Applications (1194.22) http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/guide-to-the-section-508-standards/web-based-intranet-and-internet-information-and-applications-1194-22 , Telecommunications Products (1194.23) http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/guide-to-the-section-508-standards/telecommunications-products-1194-23 , Video and Multimedia Products (1194.24) http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/guide-to-the-section-508-standards/video-and-multimedia-products-1194-24 , Self Contained, Closed Products (1194.25) http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/guide-to-the-section-508-standards/self-contained,-closed-products-1194-25 , Desktop and Portable Computers (1194.26) http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/guide-to-the-section-508-standards/desktop-and-portable-computers-1194-26 .

16. Energy Star and Electronic Product Environmental Assessment Tool (EPEAT)
16.1 Executive Order 13693 Federal Leadership in Environmental, Energy, and Economic Performance, 19 March 2015. https://www.fedcenter.gov/programs/eo13693/

16.2 Energy Star Program Requirements for Computers, Version 6.1 , 20 Oct 2014 http://www.energystar.gov/sites/default/files/FINAL%20Version%206.1%20Computer%20Program%20Requirements%20%28Rev%20Oct-2014%29_PTECMAX_Clean_0.pdf

16.3 Energy Star Program Requirements for Displays, Version 6.0, 20 Oct 2014 http://www.energystar.gov/sites/default/files/FINAL%20Version%206.0%20Display%20Program%20Requirements%20%28Rev%20Oct-2014%29_0.pdf

16.4 Energy Star Program Requirements for Imaging Equipment.
http://www.energystar.gov/sites/default/files/FINAL%20Version%202.0%20Imaging%20Equipment%20Program%20Requirements%20%28Rev%20Oct-2014%29_0.pdf

16.5 Energy Star Program Requirements for Televisions, Version 7.0, 30 Oct 2015
http://www.energystar.gov/sites/default/files/FINAL%20Version%207.0%20Television%20Program%20Requirements%20%28Dec-2014%29_0.pdf

16.6 Energy Star Program Requirements for Data Center Storage, Version 1.0,20 March 2014,
http://www.energystar.gov/sites/default/files/specs//private/Storage%20V1%200%20Final%20Program%20Requirements%20%28Rev%20Mar-2014%29.pdf

16.7 Energy Star Program Requirements for Enterprise Servers, Version 2.0, 28 Oct 2013,
http://www.energystar.gov/sites/default/files/specs//private/ENERGY%20STAR%20Computer%20Servers%20Program%20Requirements%20%28Oct-2013%29.pdf

16.8 Electronic Product Environmental Assessment Tool (EPEAT), http://www.epeat.net/

16.9 Executive Order 13423, Strengthening Federal Environmental, Energy, and Transportation Management 24 January 2007,
http://www.gsa.gov/portal/content/102452

16.10 Federal Acquisition Regulation; FAR Case 2006–030, Electronic Products Environmental Assessment Tool. Federal Register / Vol. 74, No. 10 / Thursday, January 15, 2009 / Rules and Regulations (EPEAT), http://www.epa.gov/oppt/epp/pubs/guidance/fr74no10.pdf

17. Other Regulatory and Commercial Requirements
17.1 Distributed Management Task Force Desktop Management Interface Specification (DMI Version 2.0.1s)
http://www.dmtf.org/standards/documents/DMI/DSP0005.pdf

17.2 Trusted Computing Group, Trusted Platform Module (TPM v1.2)
https://www.trustedcomputinggroup.org/developers/trusted_platform_module/specifications

17.3 FCC Part 15 Class B http://www.gpo.gov/fdsys/pkg/CFR-2009-title47-vol1/pdf/CFR-2009-title47-vol1-part15.pdf

17.4 Electromagnetic Compatibility (EMC) Directive 89/336/EEC http://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/electromagnetic-compatibility/index_en.htm

18. System Security
18.1 Security requirements that shall be accomplished by the Contractor will be per the Risk Management Framework (RMF) for DoD Information Technology (IT), DoD Instruction 8510.01, 12 March 2014 (http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf). The Contractor shall transmit and deliver any classified material/reports IAW the National Industrial Security Program Operations Manual (NISPOM) and the Industrial Security Regulation (DoD 5220.22-R). Individual system security requirements shall be accomplished as specified in the Task/Delivery Order.