		all				
*Standard Distribution: 1 copy of the transmittal letter without the deliverable to the Contracting Officer; 1 copy of the transmittal letter with the deliverable to the Primary COR.						

Explanation of Terms:
PWS Task# - State the task from Paragraph 6 of the PWS that requires this deliverable.
Deliverable Title - State the title of the deliverable (e.g., Assessment Report, Integration Plan, etc.).
Format - You may either provide Government-specified format or contractor-determined format. It is the customer's option to either specify an existing Data Item Description (DID) for each deliverable OR allow the contractor to deliver in contractor-determined format. If no DID is specified for a deliverable, that item will be delivered in contractor-determined format. If you require a deliverable format, specify in this column (e.g., "one electronic copy in Microsoft Word 97 and one hard copy").
Due Date - Self-explanatory (It is NOT allowable to use "as required" as a deliverable due date.)
Frequency & Remarks: For items that have a frequency, state the appropriate frequency (e.g., "monthly on the 10th work day," etc. It is NOT allowable to use "as required".)

12. Security Requirements.

All security requirements are specified in the Contract Security Classification Specification, DD Form 254. The highest level of security for this effort is SECRET. This section shall be considered a supplement to block 13 of the Government provided DD 254. The following security requirements shall apply to this effort.

12.1 Facility Security Clearance.

The Contractor shall also have access to Communication Security (COMSEC), For Official Use Only, and security classification guide information. in performing the contract the Contractor will also have access to classified information at the Contractor's facility; will be able to receive and generate classified material; fabricate, modify, and store classified hardware; require a COMSEC account, have OPSEC requirements, and be authorized to use the defense courier services.

Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with— (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); any revisions to DoD 5220.22-M.

12.2 Security Clearance and IT Level.

All personnel performing on this contract must be U.S. citizens. Those personnel requiring access to Secret information require at a minimum an interim Secret security clearance. Per AR 381-12 Threat Awareness and Reporting Program (TARP), contractor employees with security clearances must complete annual TARP training: http://cdsetrain.dtic.mil/thwarting/. Certifications will be submitted to the COR on an annual basis.

12.3 Investigation Requirements.

All personnel requiring access to Secret information, under this contract must undergo a favorably adjudicated National Agency Check, Local Agency Check and Credit Check (NACLC) as a minimum investigation. The NACLC will be maintained current within 10-years and requests for Secret Periodic Reviews (SPRs) will be initiated ninety (90) days prior to the 10-year anniversary date of the previous NACLC or SPR.

12.4 Security Contacts.

The applicable Security contacts for this Contract are:

Name:	TBD
Organization:	U.S. Army, PM MC

DODAAC:	W80YBY
Address:	PM MC W6DR PEO C3T BLDG 6007 COMBAT DRIVE ABERDEEN PROVING GROUND, MD 21005-1846
Phone Number:	TBD
Fax Number:	TBD
E-Mail Address:	TBD

13. Government-Furnished Equipment (GFE)/Government-Furnished Information (GFI). All GFE for this contract is captured in the AFATDS 7.0 GFE attachment to the contract. See RFP attachment J-4.

14. Other Pertinent Information or Special Considerations. *Include any special considerations or unique requirements necessary to accomplish the contract/TO (e.g., "specialized experience with UNIX") and/or any additional information that will be helpful in determining reasonable approaches and cost estimates for the contract/TO. As appropriate, this section needs to contain:*

a. Identification of Possible Follow-on Work. Not applicable.

b. Identification of Potential Conflicts of Interest (COI). *Organizational COI is a situation where because of other relationships or activities a person (company) is unable or potentially unable to render impartial assistance or advice to the Government or cannot objectively perform contract work or has an unfair competitive advantage. FAR 9.502 states that "an organization COI may result when factors create an actual or potential conflict of interest on an instant contract, or when the nature of the work to be performed on the instant contract creates an actual or potential COI on a future acquisition." An organizational COI exists when the nature of the work to be performed may, without some restriction on future activities, (1) result in an unfair competitive advantage to the contractor on other contracts or (2) impair the contractor's objectivity in performing the contract work. The primary burden is on the contractor to identify any organizational COI, however, the Government has the responsibility to identify and evaluate such conflicts.*

c. Identification of Non-Disclosure Requirements. Contractor personnel working under this contract with access to Controlled Unclassified Information (CUI) or Secret information shall be required to sign Non-Disclosure Agreements (NDAs). All NDAs shall be maintained by the Contractor and submitted to the COR prior to accessing any CUI or Secret data.

d. Packaging, Packing and Shipping Instructions. Not Applicable.

e. Inspection and Acceptance Criteria. As stated in Section E of the contract.

f. Property Accountability. Not Applicable.

g. DoD Enterprise Service Management Framework (DESMF) Compliance. All IT service requirements contained within this SOO shall be conducted in accordance with the DESMF which can be accessed at https://community.apan.org/esmf_consortium_working_groups/m/desmf_ed_ii/default.aspx.

h. Supply Chain Risk Management (SCRM). Not Applicable.

15. Section 508 Accessibility Standards. Not applicable, AFATDS is exempt from Section 508 compliance as it is a National Security System.

SECTION C

Section C-Description /specification /statement of work

Contractor Developed Performance Work Statement, Integrated Master Plan, and Contractor Work Breakdown Structure will incorporated into the resultant contract.

SECTION D

Section D - Packaging and Marking

Not Applicable

SECTION E

Section E-Inspection and Acceptance

E.1. ACCESS TO RECORD, DATA AND FACILITIES.

The Contractor shall permit the contracting officer (KO), contracting officer's representative (COR) and/or designated representative's access at any reasonable time to all records, data and facilities used in performance of the contemplated services.

E.2. DATA FORMAT, INSPECTION AND ACCEPTANCE.

Inspection and acceptance requirements for data items will be specified on separate DD Forms 1423 or incorporated into the deliverables schedule under this contract. The format of data items shall be submitted as specified in the DD Form 1423 or contract.

E.3. INSPECTION AND ACCEPTANCE

Inspection and acceptance for all Contract and or Subline Items shall be accomplished by the Program Manager, COR and/or designated Government representative.

INSPECTION AND ACCEPTANCE TERMS

Supplies/services will be inspected/accepted at:

CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
0001	N/A	N/A	N/A	Government
0002	N/A	N/A	N/A	Government
0003	N/A	N/A	N/A	Government
0004	N/A	N/A	N/A	Government
0005	N/A	N/A	N/A	Government
0006	N/A	N/A	N/A	Government
0007	N/A	N/A	N/A	Government
1006	N/A	N/A	N/A	Government
1007	N/A	N/A	N/A	Government
2006	N/A	N/A	N/A	Government
2007	N/A	N/A	N/A	Government
3006	N/A	N/A	N/A	Government
3007	N/A	N/A	N/A	Government
4006	N/A	N/A	N/A	Government
4007	N/A	N/A	N/A	Government
9999	N/A	N/A	N/A	Government

CLAUSES INCORPORATED BY REFERENCE

52.246-5	Inspection Of Services Cost-Reimbursement	APR 1984

Section F - Deliveries or Performance

SECTION F

Section F

CLIN PERFORMANCE PERIODS.

The respective performance periods for CLINs identified in Section B is as follows:

CLIN Number	Period of Performance
0001	Date of Award through 26 months
0002	*Effective Date of Optional CLIN through 26 months
0006	Date of Award through 12 months
0007	Date of Award through 12 months
1006-1007	Effective Date of Option Period through 12 months
2006-2007	Effective Date of Option Period through 12 months
3006-3007	Effective Date of Option Period through 12 months
4006-4007	Effective Date of Option Period through 12 months

*Optional CLIN 0002 will be exercised at the 27th month, as a follow-on to CLIN 0001, if required.

AFATDS 7.0 Modernization/Development	Year 1	Year 2	Year 3	Year 4	Year 5
CLIN 0001-Modernization/Development Baseline	12 mons	12 mons	2 mons		
CLIN 0002-Modernization/Development Follow-On			10 mons	12 mons	4 mons
CLIN 0006-Engineering Support	12 mons				
CLIN 0007-Other Direct Cost (ODC)	12 mons				
CLIN 1006-Engineering Support		12 mons			
CLIN 1007-ODC		12 mons			
CLIN 2006-Engineering Support			12 mons		
CLIN 2007-ODC			12 mons		
CLIN 3006-Engineering Support				12 mons	
CLIN 3007-ODC				12 mons	
CLIN 4006-Engineering Support					12 mons
CLIN 4007-ODC					12 mons

DELIVERY INFORMATION

CLIN	DELIVERY DATE	QUANTITY	SHIP TO ADDRESS	DODAAC

0001	N/A	N/A	N/A	N/A
0002	N/A	N/A	N/A	N/A
0003	N/A	N/A	N/A	N/A
0004	N/A	N/A	N/A	N/A
0005	N/A	N/A	N/A	N/A
0006	N/A	N/A	N/A	N/A
0007	N/A	N/A	N/A	N/A
1006	N/A	N/A	N/A	N/A
1007	N/A	N/A	N/A	N/A
2006	N/A	N/A	N/A	N/A
2007	N/A	N/A	N/A	N/A
3006	N/A	N/A	N/A	N/A
3007	N/A	N/A	N/A	N/A
4006	N/A	N/A	N/A	N/A
4007	N/A	N/A	N/A	N/A
9999	N/A	N/A	N/A	N/A

CLAUSES INCORPORATED BY REFERENCE

52.242-15	Stop-Work Order	AUG 1989
52.242-15 Alt I	Stop-Work Order (Aug 1989) - Alternate I	APR 1984

SECTION G

Section G-Contract Administration Data

G.1. FEE BILLING INSTRUCTIONS

a. With the exception of the provision fee listed in paragraph 7.1 of the Incentive Plan, Attachment J-3 (Incentive #1), the Government will perform an incentive review prior to payment of any incentive fees.

b. In incentive#2, the Government will review and make a final determination for the fee earned in performance of engineering releases and provide the results to the contracting officer. If approved, the contractor will be notified of the approval to invoice against the incentive CLIN.

CLAUSES INCORPORATED BY REFERENCE

252.204-7006	Billing Instructions	OCT 2005
252.232-7003	Electronic Submission of Payment Requests and Receiving Reports	JUN 2012

CLAUSES INCORPORATED BY FULL TEXT

52.204-9000 POINTS OF CONTACT (AUG 2005)

Contracting Officer
Name: KAREN KINZEL
Organization/Office Symbol: DISA/DITCO/PL83XX
Phone No.: 618-229-9243
E-Mail Address: karen.m.kinzel2.civ@mail.mil

Contract Specialist
Name: DUSTIE THOMPSON
Organization/Office Symbol: DISA/DITCO/PL83XX
Phone No.: 618-229-9127
E-Mail Address: dustie.m.thompson.civ@mail.mil

COR/Mission Partner Point of Contact (Note: To be filled in upon contract award)

Name:
Organization/Office Symbol:
Phone No.:
E-Mail Address:

Contractor Point of Contact
Contractor Legal Business Name:
DUNS:
CAGE CODE:
Contractor POC:
E-Mail Address:
Phone Number:
Fax Number:

(End of clause)

252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (MAY 2013)

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

Department of Defense Activity Address Code (DoDAAC) is a six position code that uniquely identifies a unit, activity, or organization.

Document type means the type of payment request or receiving report available for creation in Wide Area WorkFlow (WAWF).

Local processing office (LPO) is the office responsible for payment certification when payment certification is done external to the entitlement system.

(b) Electronic invoicing. The WAWF system is the method to electronically process vendor payment requests and receiving reports, as authorized by DFARS 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(c) WAWF access. To access WAWF, the Contractor shall--

(1) Have a designated electronic business point of contact in the System for Award Management at https://www.acquisition.gov; and

(2) Be registered to use WAWF at https://wawf.eb.mil/ following the step-by-step procedures for self-registration available at this Web site.

(d) WAWF training. The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the “Web Based Training” link on the WAWF home page at https://wawf.eb.mil/.

(e) WAWF methods of document submission. Document submissions may be via Web entry, Electronic Data Interchange, or File Transfer Protocol.

(f) WAWF payment instructions. The Contractor must use the following information when submitting payment requests and receiving reports in WAWF for this contract/order:

(1) Document type. The Contractor shall use the following document type(s).

TBD

(Contracting Officer: Insert applicable document type(s). Note: If a “Combo” document type is identified but not supportable by the Contractor's business systems, an “Invoice” (stand-alone) and “Receiving Report” (stand-alone) document type may be used instead.)

(2) Inspection/acceptance location. The Contractor shall select the following inspection/acceptance location(s) in WAWF, as specified by the contracting officer.

TBD

(Contracting Officer: Insert inspection and acceptance locations or “Not applicable”.)

(3) Document routing. The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

Routing Data Table*

Field Name in WAWF	Data to be entered in WAWF
Pay Official DoDAAC	TBD
Issue By DoDAAC	TBD
Admin DoDAAC	TBD
Inspect By DoDAAC	TBD
Ship To Code	N/A
Ship From Code	N/A
Mark For Code	N/A
Service Approver (DoDAAC)	TBD
Service Acceptor (DoDAAC)	TBD
Accept at Other DoDAAC	TBD
LPO DoDAAC	TBD
DCAA Auditor DoDAAC	N/A
Other DoDAAC(s)	N/A

(*Contracting Officer: Insert applicable DoDAAC information or “See schedule” if multiple ship to/acceptance locations apply, or “Not applicable.”)

(4) Payment request and supporting documentation. The Contractor shall ensure a payment request includes appropriate contract line item and subline item descriptions of the work performed or supplies delivered, unit price/cost per unit, fee (if applicable), and all relevant back-up documentation, as defined in DFARS Appendix F, (e.g. timesheets) in support of each payment request.

(5) WAWF email notifications. The Contractor shall enter the email address identified below in the “Send Additional Email Notifications” field of WAWF once a document is submitted in the system.
TBD

(g) WAWF point of contact. (1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.

TBD

(2) For technical WAWF help, contact the WAWF helpdesk at 866-618-5988.

(End of clause)

Additional Accounting and Appropriation Data

97X4930.5F20 000 C1013 0 068142 2F

CLIN/SubCLIN	Purchase Request Number	Obligated Amount

SECTION H
Section H-Special Contract Requirements

H.1 SECURITY CLEARANCE

The appropriate security requirements are required upon contract award See DD Form 254, Section J, Attachment J-2

H.2 MATERIAL RIGHTS

c. The Government requires all non-commercial software and software documentation provided under the AFATDS contract be furnished to the Government with unlimited rights and become the property of the Government at completion of the contract. Note that integration of COTS software shall not be considered contractor development of software at private expense. Any exception to this must be addressed in the contractor's proposal. Contractors shall obtain the Government's approval of non-free and open source (non-FOSS) and COTS items prior to their incorporation.

d. The Government requires all materials (hardware, manuals, documentation, consumables, etc.) provided under this contract to become the property of the Government at completion of the contract.

e. Software and all other materials that shall become the property of the Government, as stated above, at completion of the contract will be listed in the contractor'sproposal.

H.3 RELEASE OF NEWS INFORMATION

No news release (including photographs and films, public announcements, denial or confirmation of same) on any part of the subject matter of this contract or any phase of any program hereunder shall be made without the prior written approval of the Contracting Officer and DISA Public Affairs Office (PAO), and if Congressionally-related, DISA Congressional Affairs (CA). See also Section I, DFARS clause 252.204 7000 "Disclosure of Information".

H.4 ANNUAL PERFORMANCE ASSESSMENT

a. The COR will evaluate and document the contractor's performance on an annual basis in a web-based Contractor Performance Assessment Reporting System (CPARS) (or similar). The COR will forward the rating of contractor's performance to the Assessing Official for approval. The Assessing Official then forwards the rating to the Contracting Officer, who will forward it to the contractor for review. The contractor may not change the rating. The contractor shall either concur, concur with comments, or not concur with comments, and return the evaluation to the Contracting Officer within 30 calendar days.

b. Past performance information is relevant information regarding the contractor's actions under previously awarded contracts. The written performance evaluation will state whether the services/supplies met the Government's stated requirements and specifications and if they were performed/delivered on time. It includes, for example, the contractor's record of conforming to contract requirements and to standards of good workmanship; the contractor's adherence to contract schedules, including the administrative aspects of performance; the contractor's history of reasonable and cooperative behavior and commitment to customer satisfaction; and generally, the contractor's business-like concern for the interest of the customer. This evaluation may be either printed or electronic format, as defined by the Government.

c. The evaluation of the contractor's performance will be used as a criterion for exercising any unexercised option. The evaluation will also be used by DISA and other Government agencies as source selection information to support future Government procurements.

H.5 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)/OCI MITIGATION PLAN

a. An organizational conflict of interest means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage. The Government seeks to acquire unbiased advice and/or goods and services from offerors/contractors that are free from, or have mitigated, Organizational Conflicts of Interest , as defined in FAR 2.101, relating to this contract.

b. In order for the Government to try to prevent an OCI relating to this contract, the parties to this contract agree that the contractor's future contracting with the Government may be restricted as outlined in FAR Subpart 9.5, if the offeror/contractor and DISA are unable to avoid, neutralize, or mitigate actual or potential OCI before contract award.

c. DISA will not automatically exclude a vendor from a competitive acquisition due to an actual or potential OCI. The Contracting Office is committed to working with potential vendors to eliminate or mitigate actual and potential OCI situations, without detriment to the integrity of the competitive process, the DISA mission, or the legitimate business interests of the vendor community.

d. If the offeror or contractor is aware, or should have been aware, of an OCI before award of this contract or any task under against the contract, and does not fully disclose that conflict to the Contracting Officer, the Government may terminate the contractor for default.

e. The offeror or contractor, by submitting an offer and/or signing the contract, warrants that it is not now aware of any actual or potential OCI relating to this contract.

f. After contract award, the contractor shall have an ongoing obligation to make "a prompt and full disclosure" to the Contracting Officer of any OCI that arises during the performance of the contract, as well as newly discovered conflicts that existed before contract award.

g. The OCI Mitigation Plan shall become part of the resultant contract and the contractor shall update its OCI Mitigation Plan within 30 days of any changes to the legal construct of the organization, subcontractor changes, or significant management or ownership changes that would result in an actual or potential OCI under this contract.

H.6 52.237-9001 Enterprise-wide Contractor Manpower Reporting Application (eCMRA) Reporting.

ENTERPRISE-WIDE CONTRACTOR MANPOWER REPORTING APPLICATION (eCMRA) REPORTING (JAN 2015)

The contractor shall ensure ALL contractor labor hours including subcontractor, at all levels/tiers, labor hours required for the performance of services provided under this contract are reported via a secure data collection site.

The contractor and all subcontractors, at all levels/tiers, providing direct labor under this contract shall report complete and accurate data for the labor executed during the period of performance during each Government fiscal year (FY), which runs from October 1 to September 30. The Contractor shall input the data into the appropriate eCMRA reporting tool, which can be accessed via a secure web site at http://www.ecmra.mil/. There are four separate eCMRA tools: Army, Air Force, Navy and All Other Defense Components. The appropriate eCMRA reporting tool to use is determined by the requiring activity being supported (e.g., if DISA awards a contract for an Air Force requiring activity, the contractor shall load the required reporting data in the "Department of Air Force CMRA" tool). While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. The contractor shall completely fill in all required data fields. The contractor shall enter initial data into the appropriate eCMRA tool to establish the basic contract record no later than 15 working days after receipt of contract award or contract modification incorporating this clause. The contractor shall notify the COR when the basic contract record has been established in the appropriate eCMRA tool.

eCMRA User Manuals and Frequently Asked Questions (FAQs) are available at http://www.ecmra.mil/

Contractors may direct technical questions to the eCMRA help desk at usaf.pentagon.saf-aq.mbx.cmra-help-desk-dod@mail.mil

H.7 252.225-7048 Export-Controlled Items.

EXPORT CONTROLLED ITEMS (JUNE 2013)

(a) *Definition.* "Export-controlled items," as used in this clause, means items subject to the Export Administration Regulations (EAR) (15 CFR Parts 730-774) or the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130). The term includes:

(1) "Defense items," defined in the Arms Export Control Act, 22 U.S.C. 2778(j)(4)(A), as defense articles, defense services, and related technical data, and further defined in the ITAR, 22 CFR Part 120.

(2) "Items," defined in the EAR as "commodities", "software", and "technology," terms that are also defined in the EAR, 15 CFR 772.1.

(b) The Contractor shall comply with all applicable laws and regulations regarding export-controlled items, including, but not limited to, the requirement for contractors to register with the Department of State in accordance with the ITAR. The Contractor shall consult with the Department of State regarding any questions relating to compliance with the ITAR and shall consult with the Department of Commerce regarding any questions relating to compliance with the EAR.

(c) The Contractor's responsibility to comply with all applicable laws and regulations regarding export-controlled items exists independent of, and is not established or limited by, the information provided by this clause.

(d) Nothing in the terms of this contract adds, changes, supersedes, or waives any of the requirements of applicable Federal laws, Executive orders, and regulations, including but not limited to—

(1) The Export Administration Act of 1979, as amended (50 U.S.C. App. 2401, *et seq*.);

(2) The Arms Export Control Act (22 U.S.C. 2751, *et seq*.);

(3) The International Emergency Economic Powers Act (50 U.S.C. 1701, et seq.);

(4) The Export Administration Regulations (15 CFR Parts 730-774);

(5) The International Traffic in Arms Regulations (22 CFR Parts 120-130); and

(6) Executive Order 13222, as extended.

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

(End of clause)

H.8 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.

As prescribed in 204.7304(c), use the following clause:

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2015)

(a) *Definitions*. As used in this clause—

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

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

"Contractor information system" means an information system belonging to, or operated by or for, the Contractor.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Covered contractor information system" means an information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

"Covered defense information" means unclassified information that—

(i) Is—

(A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

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

(ii) Falls in any of the following categories:

(A) *Controlled technical information.*

(B) *Critical information (operations security)*. Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(C) *Export control*. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(D) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

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

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

“Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

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

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

"Rapid(ly) report(ing)" means within 72 hours of discovery of any cyber incident.

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

(b) *Adequate security*. The Contractor shall provide adequate security for all covered defense information on all covered contractor information systems that support the performance of work under this contract. To provide adequate security, the Contractor shall—

(1) Implement information systems security protections on all covered contractor information systems including, at a minimum—

(i) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government—

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

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

(ii) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1)(i) of this clause—

(A) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or

(B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and

(2) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in

paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

(c) *Cyber incident reporting requirement.*

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.

(2) *Cyber incident report.* The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.

(3) *Medium assurance certificate requirement*. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see http://iase.disa.mil/pki/eca/Pages/index.aspx.

(d) *Malicious software*. The Contractor or subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by the Contracting Officer.

(e) *Media preservation and protection*. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) *Access to additional information or equipment necessary for forensic analysis*. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) *Cyber incident damage assessment activities*. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) *DoD safeguarding and use of contractor attributional/proprietary information*. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) *Use and release of contractor attributional/proprietary information not created by or for DoD*. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

(1) To entities with missions that may be affected by such information;

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

(3) To Government entities that conduct counterintelligence or law enforcement investigations;

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) *Use and release of contractor attributional/proprietary information created by or for DoD*. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) *Other safeguarding or reporting requirements*. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) *Subcontracts*. The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve a covered contractor information system, including subcontracts for commercial items, without alteration, except to identify the parties; and

(2) When this clause is included in a subcontract, require subcontractors to rapidly report cyber incidents directly to DoD at http://dibnet.dod.mil and the prime Contractor. This includes providing the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable.

(End of clause)

CLAUSES INCORPORATED BY REFERENCE

252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting.	DEC 2015
252.225-7048	Export-Controlled Items	JUN 2013
252.227-7013	Rights in Technical Data--Noncommercial Items	FEB 2014
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	FEB 2014
252.227-7019	Validation of Asserted Restrictions--Computer Software	SEP 2011
252.227-7028	Technical Data or Computer Software Previously Delivered to the Government	JUN 1995
252.227-7030	Technical Data--Withholding Of Payment	MAR 2000
252.227-7037	Validation of Restrictive Markings on Technical Data	JUN 2013
252.234-7001	Notice of Earned Value Management System	APR 2008

252.234-7002 Earned Value Management System MAY 2011

CLAUSES INCORPORATED BY FULL TEXT

52.237-9001 ENTERPRISE-WIDE CONTRACTOR MANPOWER REPORTING APPLICATION (eCMRA) REPORTING (JAN 2015)

The contractor shall ensure ALL contractor labor hours including subcontractor, at all levels/tiers, labor hours required for the performance of services provided under this contract are reported via a secure data collection site.

The contractor and all subcontractors, at all levels/tiers, providing direct labor under this contract shall report complete and accurate data for the labor executed during the period of performance during each Government fiscal year (FY), which runs from October 1 to September 30. The Contractor shall input the data into the appropriate eCMRA reporting tool, which can be accessed via a secure web site at http://www.ecmra.mil/. There are four separate eCMRA tools: Army, Air Force, Navy and All Other Defense Components. The appropriate eCMRA reporting tool to use is determined by the requiring activity being supported (e.g., if DISA awards a contract for an Air Force requiring activity, the contractor shall load the required reporting data in the "Department of Air Force CMRA" tool). While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. The contractor shall completely fill in all required data fields. The contractor shall enter initial data into the appropriate eCMRA tool to establish the basic contract record no later than 15 working days after receipt of contract award or contract modification incorporating this clause. The contractor shall notify the COR when the basic contract record has been established in the appropriate eCMRA tool.

eCMRA User Manuals and Frequently Asked Questions (FAQs) are available at http://www.ecmra.mil/

Contractors may direct technical questions to the eCMRA help desk at usaf.pentagon.saf-aq.mbx.cmra-help-desk-dod@mail.mil
(End of clause)

252.227-7016 RIGHTS IN BID OR PROPOSAL INFORMATION (JAN 2011)

(a) Definitions.

(1) For contracts that require the delivery of technical data, the terms "technical data" and "computer software" are defined in the Rights in Technical Data--Noncommercial Item clause of this contract or, if this is a contract awarded under the Small Business Innovation Research Program, the Rights in Noncommercial Technical Data and Computer Software--Small Business Innovation Research (SBIR) Program clause of this contract.

(2) For contracts that do not require the delivery of technical data, the term "computer software" is defined in the Rights in Noncommercial Computer and Noncommercial Computer Software Documentation clause of this contract or, if this is a contract awarded under the Small Business Innovation Research Program, the Rights in Noncommercial Technical Data and Computer Software--Small Business Innovation Research (SBIR) Program clause of this contract.

(b) Government rights to contract award. By submission of its offer, the Offeror agrees that the Government--

(1) May reproduce the bid or proposal, or any portions thereof, to the extent necessary to evaluate the offer.

(2) Except as provided in paragraph (d) of this clause, shall use information contained in the bid or proposal only for evaluational purposes and shall not disclose, directly or indirectly, such information to any person including potential evaluators, unless that person has been authorized by the head of the agency, his or her designee, or the Contracting Officer to receive such information.

(c) Government rights subsequent to contract award--The Contractor agrees--

(1) Except as provided in paragraphs (c)((2), (d), and (e) of this clause, the Government shall have the rights to use, modify, reproduce, release, perform, display, or disclose information contained in the Contractor's bid or proposal within the Government. The Government shall not release, perform, display, or disclose such information outside the Government without the Contractor's written permission.

(2) The Government's right to use, modify, reproduce, release, perform, display, or disclose information that is technical data or computer software required to be delivered under this contract are determined by the Rights in Technical Data--Noncommercial Items, Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation, or Rights in Noncommercial Technical Data and Computer Software--Small Business Innovation Research (SBIR) Program clause(s) of this contract.

(d) Government-furnished information. The Government's rights with respect to technical data or computer software contained in the Contractor's bid or proposal that were provided to the Contractor by the Government are subject only to restrictions on use, modification, reproduction, release, performance, display, or disclosure, if any, imposed by the developer or licensor of such data or software.

(e) Information available without restrictions. The Government's rights to use, modify, reproduce, release, perform, display, or, disclose information contained in a bid or proposal, including technical data or computer software, and to permit others to do so, shall not be restricted in any manner if such information has been released or disclosed to the Government or to other persons without restrictions other than a release or disclosure resulting from the sale, transfer, or other assignment of interest in the information to another party or the sale or transfer of some or all of a business entity or its assets to another party.

(f) Flowdown. Contractor shall include this clause in all subcontracts or similar contractual instruments and require its subcontractors or suppliers to do so without alteration, except to identify the parties.

(End of clause)

Section I - Contract Clauses

CLAUSES INCORPORATED BY REFERENCE

52.202-1	Definitions	NOV 2013
52.203-3	Gratuities	APR 1984
52.203-5	Covenant Against Contingent Fees	MAY 2014
52.203-6	Restrictions On Subcontractor Sales To The Government	SEP 2006
52.203-7	Anti-Kickback Procedures	MAY 2014
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	MAY 2014
52.203-10	Price Or Fee Adjustment For Illegal Or Improper Activity	MAY 2014
52.203-12	Limitation On Payments To Influence Certain Federal Transactions	OCT 2010
52.203-17	Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights	APR 2014
52.204-4	Printed or Copied Double-Sided on Postconsumer Fiber Content Paper	MAY 2011
52.204-5	Women-Owned Business (Other Than Small Business)	OCT 2014
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	OCT 2015
52.204-19	Incorporation by Reference of Representations and Certifications.	DEC 2014
52.209-6	Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, or Proposed for Debarment	OCT 2015
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	JUL 2013
52.209-9000	ORGANIZATIONAL AND CONSULTANT CONFLICTS OF INTEREST (OCCI) (DEC 2014)	DEC 2014
52.215-2	Audit and Records--Negotiation	OCT 2010
52.215-8	Order of Precedence--Uniform Contract Format	OCT 1997
52.215-11	Price Reduction for Defective Certified Cost or Pricing Data--Modifications	AUG 2011
52.215-13	Subcontractor Certified Cost or Pricing Data--Modifications	OCT 2010
52.215-15	Pension Adjustments and Asset Reversions	OCT 2010
52.215-16	Facilities Capital Cost of Money	JUN 2003
52.215-17	Waiver of Facilities Capital Cost of Money	OCT 1997
52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other than Pensions	JUL 2005
52.215-19	Notification of Ownership Changes	OCT 1997
52.215-21	Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data -- Modifications	OCT 2010
52.215-23	Limitations on Pass-Through Charges	OCT 2009
52.215-23 Alt I	Limitations on Pass-Through Charges (Oct 2009) - Alternate I	OCT 2009
52.216-7	Allowable Cost And Payment	JUN 2013
52.216-8	Fixed Fee	JUN 2011
52.216-10	Incentive Fee	JUN 2011
52.219-1	Small Business Program Representations	OCT 2014
52.219-1 Alt I	Small Business Program Representations (Sept 2015) Alternate I	SEP 2015
52.219-4	Notice of Price Evaluation Preference for HUBZone Small Business Concerns	OCT 2014

52.219-8	Utilization of Small Business Concerns	OCT 2014
52.219-9 (Dev)	Small Business Subcontracting Plan (Deviation 2013-O0014)	OCT 2015
52.219-16	Liquidated Damages-Subcontracting Plan	JAN 1999
52.219-28	Post-Award Small Business Program Rerepresentation	JUL 2013
52.222-2	Payment For Overtime Premiums	JUL 1990
52.222-3	Convict Labor	JUN 2003
52.222-21	Prohibition Of Segregated Facilities	APR 2015
52.222-26	Equal Opportunity	APR 2015
52.222-35	Equal Opportunity for Veterans	OCT 2015
52.222-36	Equal Opportunity for Workers with Disabilities	JUL 2014
52.222-37	Employment Reports on Veterans	OCT 2015
52.222-40	Notification of Employee Rights Under the National Labor Relations Act	DEC 2010
52.222-50	Combating Trafficking in Persons	MAR 2015
52.222-54	Employment Eligibility Verification	OCT 2015
52.223-6	Drug-Free Workplace	MAY 2001
52.223-18	Encouraging Contractor Policies To Ban Text Messaging While Driving	AUG 2011
52.224-1	Privacy Act Notification	APR 1984
52.224-2	Privacy Act	APR 1984
52.225-13	Restrictions on Certain Foreign Purchases	JUN 2008
52.227-1	Authorization and Consent	DEC 2007
52.227-2	Notice And Assistance Regarding Patent And Copyright Infringement	DEC 2007
52.228-7	Insurance--Liability To Third Persons	MAR 1996
52.230-2	Cost Accounting Standards	OCT 2015
52.230-3	Disclosure And Consistency Of Cost Accounting Practices	OCT 2015
52.230-6	Administration of Cost Accounting Standards	JUN 2010
52.232-9	Limitation On Withholding Of Payments	APR 1984
52.232-18	Availability Of Funds	APR 1984
52.232-20	Limitation Of Cost	APR 1984
52.232-22	Limitation Of Funds	APR 1984
52.232-23	Assignment Of Claims	MAY 2014
52.232-23 Alt I	Assignment of Claims (May 2014) - Alternate I	APR 1984
52.232-25	Prompt Payment	JUL 2013
52.232-33	Payment by Electronic Funds Transfer--System for Award Management	JUL 2013
52.232-35	Designation of Office for Government Receipt of Electronic Funds Transfer Information	JUL 2013
52.232-39	Unenforceability of Unauthorized Obligations	JUN 2013
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.233-1	Disputes	MAY 2014
52.233-1 Alt I	Disputes (May 2014) - Alternate I	DEC 1991
52.233-2	Service Of Protest	SEP 2006
52.233-3 Alt I	Protest After Award (Aug 1996) - Alternate I	JUN 1985
52.233-4	Applicable Law for Breach of Contract Claim	OCT 2004
52.237-3	Continuity Of Services	JAN 1991
52.239-1	Privacy or Security Safeguards	AUG 1996
52.242-1	Notice of Intent to Disallow Costs	APR 1984
52.242-3	Penalties for Unallowable Costs	MAY 2014
52.242-4	Certification of Final Indirect Costs	JAN 1997
52.242-13	Bankruptcy	JUL 1995
52.243-2 Alt I	Changes--Cost-Reimbursement (Aug 1987) - Alternate I	APR 1984
52.243-7	Notification Of Changes	APR 1984

52.244-2	Subcontracts	OCT 2010
52.244-5	Competition In Subcontracting	DEC 1996
52.245-1	Government Property	APR 2012
52.245-9	Use And Charges	APR 2012
52.246-8	Inspection Of Research And Development Cost Reimbursement	MAY 2001
52.246-25	Limitation Of Liability--Services	FEB 1997
52.249-6	Termination (Cost Reimbursement)	MAY 2004
52.249-14	Excusable Delays	APR 1984
52.252-2	Clauses Incorporated By Reference	FEB 1998
52.252-4	Alterations in Contract	APR 1984
52.252-6	Authorized Deviations In Clauses	APR 1984
52.253-1	Computer Generated Forms	JAN 1991
252.203-7000	Requirements Relating to Compensation of Former DoD Officials	SEP 2011
252.203-7001	Prohibition On Persons Convicted of Fraud or Other Defense-Contract-Related Felonies	DEC 2008
252.203-7002	Requirement to Inform Employees of Whistleblower Rights	SEP 2013
252.203-7996 (Dev)	Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements—Representation (Deviation 2016-O0003)	OCT 2015
252.203-7997 (Dev)	Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements (Deviation 2016-O0003)	OCT 2015
252.204-7000	Disclosure Of Information	AUG 2013
252.204-7003	Control Of Government Personnel Work Product	APR 1992
252.204-7004 Alt A	System for Award Management Alternate A	FEB 2014
252.204-7008	Compliance With Safeguarding Covered Defense Information Controls	DEC 2015
252.204-7012 (Dev)	Safeguarding Covered Defense Information and Cyber Incident Reporting	OCT 2015
252.205-7000	Provision Of Information To Cooperative Agreement Holders	DEC 1991
252.209-7004	Subcontracting With Firms That Are Owned or Controlled By The Government of a Country that is a State Sponsor of Terrorism	OCT 2015
252.209-7991 (Dev)	Representation by Corporations Regarding an Unpaid Delinquent Tax Liability or a Felony Conviction under any Federal Law—Fiscal Year 2016 Appropriations. (DEVIATION 2016-O0002)	OCT 2015
252.209-7997 (Dev)	Representation by Corporations Regarding an Unpaid Delinquent Tax Liability or a Felony Conviction under any Federal Law - DoD Appropriations	JAN 2013
252.211-7007	Reporting of Government-Furnished Property	AUG 2012
252.215-7000	Pricing Adjustments	DEC 2012
252.219-7003	Small Business Subcontracting Plan (DOD Contracts)	OCT 2014
252.223-7004	Drug Free Work Force	SEP 1988
252.225-7012	Preference For Certain Domestic Commodities	FEB 2013
252.226-7001	Utilization of Indian Organizations and Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns	SEP 2004
252.227-7015	Technical Data--Commercial Items	FEB 2014
252.231-7000	Supplemental Cost Principles	DEC 1991
252.233-7001	Choice of Law (Overseas)	JUN 1997
252.235-7011	Final Scientific or Technical Report	JAN 2015
252.239-7001	Information Assurance Contractor Training and Certification	JAN 2008
252.239-7017	Notice of Supply Chain Risk	NOV 2013