

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING					
				a. FACILITY CLEARANCE REQUIRED Secret					
				b. LEVEL OF SAFEGUARDING REQUIRED None					
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>				3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>					
		a. PRIME CONTRACT NUMBER		X	a. ORIGINAL <i>(Complete date in all cases)</i>		DATE (YYYYMMDD) 20170615		
		b. SUBCONTRACT NUMBER			b. REVISED <i>(Supersedes all previous specs)</i>	REVISION NO.	DATE (YYYYMMDD)		
X	c. SOLICITATION OR OTHER NUMBER HDTRA1-16-R-0027		DUE DATE (YYYYMMDD)		c. FINAL <i>(Complete item 5 in all cases)</i>		DATE (YYYYMMDD)		
4. IS THIS A FOLLOW-ON CONTRACT? Classified material received or generated under _____				☐ YES ☒ NO. If yes, complete the following: _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.					
5. IS THIS A FINAL DD FORM 254? In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____									
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>									
a. NAME, ADDRESS, AND ZIP CODE			b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>				
7. SUBCONTRACTOR									
a. NAME, ADDRESS, AND ZIP CODE			b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>				
8. ACTUAL PERFORMANCE									
a. LOCATION			b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>				
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT									
10. CONTRACTOR WILL REQUIRE ACCESS TO:				YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION				☐	☒	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		☐	☒
b. RESTRICTED DATA				☐	☒	b. RECEIVED CLASSIFIED DOCUMENTS ONLY		☐	☒
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION				☐	☒	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		☐	☒
d. FORMERLY RESTRICTED DATA				☐	☒	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		☐	☒
e. INTELLIGENCE INFORMATION:				☐	☐	e. PERFORM SERVICES ONLY		☐	☒
(1) Sensitive Compartmented Information (SCI)				☐	☒	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		☐	☒
(2) Non-SCI				☐	☒	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		☐	☒
f. SPECIAL ACCESS INFORMATION				☐	☒	h. REQUIRE A COMSEC ACCOUNT		☐	☒
g. NATO INFORMATION				☒	☐	i. HAVE TEMPEST REQUIREMENTS		☐	☒
h. FOREIGN GOVERNMENT INFORMATION				☒	☐	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		☒	☐
i. LIMITED DISSEMINATION INFORMATION				☐	☒	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		☐	☒
j. FOR OFFICIAL USE ONLY INFORMATION				☒	☐	l. OTHER <i>(Specify)</i> See block 13		X	
k. OTHER <i>(Specify)</i>				☐	☒				

12. PUBLIC RELEASE. Any information (*classified or unclassified*) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (Specify):

Defense Threat Reduction Agency
8725 John J. Kingman Road, MS 6201
Ft. Belvoir, VA 22060-6201

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
**In the case of non-DOD User Agencies, requests for disclosure shall be submitted to that agency.*

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (*Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*)

Item 13a: The contractor shall comply with the Security Agreement (DD Form 441) including the NISPOM and any revisions to that manual, notice of which has been furnished to the contractor.

Item 13b: The contractor's employees performing work under this contract shall be U.S. citizens and been granted appropriate security clearance, based on the need for access to specific classified information. That is SECRET clearance based on favorably adjudicated National Agency Check with Law and Credit Check (NACLC) or a TOP SECRET clearance based on a Single Scope Background Investigation (SSBI) favorably adjudicated by the Defense Security Service, DoD Central Adjudicative Facility, Fort Meade, Maryland 20755.

All contractors in privileged user positions must have a completed SSBI in accordance with DOD Instruction 8500.2, "Information Assurance (IA) Implementation", 6 February 2003, paragraph E3.4.8. and Table E3.T1, prior to filling the position. Privileged users are defined as, but not limited to, persons in the following roles or positions: Information Assurance Manager/Officer, supervisors of Information Technology positions, System Administrator, maintainers of IA-enabled products such as routers, switches, firewalls, personnel performing system monitoring and testing, and personnel who issue classified Public Key Infrastructure certificates.

Item 13c: Should the contractor visit or perform work in support of this contract at any DTRA facility, the contractor shall submit proof of clearance thru JPAS to SMO Code GQDD614 or fax a Visit Authorization Request (VAR) to The DTRA Security and Counterintelligence Office (ATTN: Visitor Services). VARs shall contain the information specified in paragraph 6-104 of the NISPOM. VARs may be faxed to (703) 767-7857. The term of the VAR shall be for the period of contract performance. All classified visit request by contractors should be forwarded to the Program Manager for approval and need-to-know.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)
See block 13; Item 10j.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☐ Yes ☒ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL

b. TITLE

c. TELEPHONE (Include Area Code)

d. ADDRESS (Include Zip Code)

Defense Threat Reduction Agency
8725 John J. Kingman Road, MS 6201
Ft. Belvoir, VA 22060-6201

e. SIGNATURE

17. REQUIRED DISTRIBUTION

☒

a. CONTRACTOR

☐

b. SUBCONTRACTOR

☒

c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR

☐

d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION

☒

e. ADMINISTRATIVE CONTRACTING OFFICER

☐

f. OTHERS AS NECESSARY

BLOCK 13 (CONTINUED)

HDTRA1-16-R-0027

Item 10g: Contractor access to North Atlantic Treaty Organization (NATO) and Foreign Government Information requires a final U.S. Government clearance at the appropriate level.

Reference: DTRA Memorandum, North Atlantic Treaty Organization (NATO) Security Briefing for Secure Internet Protocol Router Network (SIPRNET) Users.

All DTRA's contractors that require a SIPRNET account must be briefed on NATO.

Item 10h: Contractor access to Foreign Government Information requires a final U.S. Government clearance at the appropriate level. Individuals should be briefed on NATO at the appropriate locations.

Item 10j: All "For Official Use Only" information shall be marked, safeguarded, transmitted, and disclosed in accordance with DoD Manual 5200.01, Volume 3, Protection of Classified Information.

Item 11j: OPSEC requirements apply. All contractors supporting this effort will receive initial and annual refresher OPSEC training and will be reminded of their continued responsibility to protect sensitive information.

At a minimum the contractor will adhere to the guidelines set forth in the Agency's OPSEC Policy Statement and Critical Information List. Additionally, the contractor will develop a Critical Information List specific to their portion of the contract work which will identify any sensitive/unclassified information which if disclosed may tip an adversary as to our intentions and/or capabilities.

Additionally, Critical Program Information (CPI) must be identified and protected IAW DoD Instruction 5200.39, Critical Program Information Protection Within the Department of Defense, July 16, 2008. CPI is the classified, highly sensitive information pertaining to a program which if compromised could cause significant degradation in mission effectiveness; shorten the expected life span of the program; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability

Item 11l: Non-US citizens will be allowed to perform work under this contract. The tasks performed by foreign nationals are not connected to any classified activities under this contract. The contractor will take appropriate measures to preclude non-US citizens from gaining access to classified material related to the contract.

The non-citizens performing work under the contract perform the following range of services:

- Administrative Services (i.e., configuration management, data management, travel itineraries, and conference/meeting planning)
- Logistics and Sustainment Planning
- Regulatory and Licensing (as it pertains to the host country)
- Scientific and Engineering Subject Matter Expertise
- Project Management Support
- Policy Expertise

Item 13e: In accordance with DTRA Policy and DTRA Instruction 5240.06, DTRA Counterintelligence Awareness, Briefing, and Reporting Programs, dated Feb 6, 2004, section 4 under Policy, all contractors working under DTRA contracts are required to comply with the following:

4.1. All DTRA contractors will receive a CI Awareness Briefing upon in-processing at DTRA. All DTRA contractors will receive an annual update of the CI Awareness Briefing.

4.2 Prior to any official travel outside the Continental United States (OCONUS) or while attending domestic or overseas meetings, conferences or symposiums where meetings with foreign nationals are expected, all DTRA contractors and personnel contracted by DTRA traveling via agency sponsored or supported activities or another DoD component, will contact the BDC or the local SC Field Office to receive a AOR Specific Travel Briefing, no more than 90 days prior to any OCONUS travel in accordance with DoD Directive 2000.16 (reference (b)).

In accordance with DODI 2000.16, Antiterrorism (AT) Standards, Standard 19; and DTRA Directive 2000.12, DTRA Antiterrorism Program, Standard 19 requires all DTRA employees and on-site DOD contractors at all DTRA locations to be provided AT Level I Training. The Security and Counterintelligence Directorate will be responsible for ensuring completion of annual AT Level I Training.

All personnel at DTRA (civilian, military, contractor or other government agency personnel), in accordance with DTRA instructions and policies, the use of personally owned electronic devices are prohibited in the DTRA facility . Unauthorized introduction of such devices into the DTRA facility constitutes a security incident; which will be followed with a security incident inquiry/report for corrective action. Unless issued/approved by DTRA, all electronic devices which require access into the DTRA facility must be coordinated and approved through the Security and Counterintelligence, Technical Security Branch.

The use of the public world-wide web/internet services is not authorized to discuss, disseminate, produce or transmit "For Official Use Only" information and classified information

All personnel at DTRA (military, civilian, contractor or other government agency personnel) that require a permanent DTRA badge or access to the DTRA LAN must receive an in-processing security brief before issuance of a DTRA badge or access to the DTRA LAN. Contractors or other government agency employees working at or supporting DTRA must be in DTRA spaces a minimum of three days per week for a DTRA permanent badge to be issued to them. Some contractors or other government agency employees working at or supporting DTRA may be required to have a DTRA LAN account. Contractors or other government agency employees working at or supporting DTRA that will be issued a DTRA permanent badge or a DTRA LAN account must in-process and receive a security briefing.

All personnel that possess a DTRA permanent badge or have access to the DTRA LAN must receive an out-processing security debrief in the event they are terminating employment, retiring, no longer supporting DTRA, being reassigned to another government agency, or will be absent from duty or employment for more than 60 consecutive days. Failure to do so may adversely affect departing personnel's security clearance and future employment.

This sentence relates to full time DTRA contractors, and personnel who are contracted by DTRA that are located in other regions, academia, etc.

All contractors that will be working in DTRA space and/or having access to the Local Area Network are required to in and out process through Personnel Security.

The signatures below indicate this contract has been coordinated with the DTRA Program Manager and the DTRA Security Operations Branch. For further assistance on the contract please contact the DTRA Program Manager listed below.

Program Manager:

Dorian Corbett DATE: 15 June 2017 Phone: 703-767-4432
Printed Name

(Signature)

Security Operations Branch:

Stefan A. Adamcik DATE: 20 June 2017 Phone: 703-767-7937
Printed Name

(Signature)