CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: TOP SECRET

b. LEVEL OF SAFEGUARDING REQUIRED: TOP SECRET

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

- ☐ a. PRIME CONTRACT NUMBER
- ☐ b. SUBCONTRACT NUMBER
- ☒ c. SOLICITATION OR OTHER NUMBER: H95001-15-R-0001 — Due Date *(YYYYMMDD)*:

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

- ☐ a. ORIGINAL *(Complete date in all cases)* — Date *(YYYYMMDD)*: 2015/08/13
- ☒ b. REVISED *(Supersedes all previous specs)* — Revision No.: 1 — Date *(YYYYMMDD)*: 2016/05/02
- ☐ c. FINAL *(Complete Item 5 in all cases)* — Date *(YYYYMMDD)*:

4. IS THIS A FOLLOW-ON CONTRACT? ☐ YES ☒ NO. If Yes complete the following

Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract

5. IS THIS A FINAL DD FORM 254? ☐ YES ☒ NO. If Yes complete the following

In response to the Contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICES *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
See Block 13, Reference Item 8.a.		

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Integrated Research & Development for Enterprise Solutions (IRES). Provides integrated solutions supporting concurrent test, training, and operations within the Missile Defense Integration and Operations Center (MDIOC) mission execution platform and enterprise communications and information technology environment.

10. THIS CONTRACT 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. RECEIVE 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 A TEMPEST REQUIREMENT	☐	☒
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 *(Specify)*	☒	☐
k. OTHER *Specify)*	☐	☒	– Restrict Access to Contractor's Unclassified Automated Information System (AIS). – Requires CNet/SIPR/JWICS		

DD Form 254, DEC 1999 *Previous editions are obsolete*

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 release shall be submitted for approval prior to release

☐ Direct ☒ Through *(Specify)*:

Missile Defense Agency/ICBP
730 Irwin Ave,
Schriever AFB, CO 80912

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 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 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 document/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*

The Contractor is required to flow-down all applicable requirements of the DD Form 254 to its Subcontractor(s).

Direct all questions pertaining to the DD Form 254 to the MDA Industrial Security office by phone at 256-313-9429, by email at MDAIndustrialSecurity@mda.mil, or by mail to MDA, ATTN: Industrial Security Office (EIR), Building 5222 Martin Road, Redstone Arsenal, AL 35898.

See Continuation Pages

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. *(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.)* ☒ Yes ☐ No

See Reference Items 10.e.(1), 10.f, 10.j, 11.j, 11.l. and 14.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. *(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.* ☐ Yes ☒ No

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)*
Derek S. Fleischmann	Acting Chief, BMDS Acquisition Security	256-313-9429

d. ADDRESS *(Include ZIP Code)*
Missile Defense Agency
5222 Martin Road
Redstone Arsenal, AL 35898

e. SIGNATURE
FLEISCHMANN.DEREK.S.1275433485
Digitally signed by FLEISCHMANN.DEREK.S.1275433485
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=MDA, cn=FLEISCHMANN.DEREK.S.1275433485
Date: 2016.05.02 13:09:01 -05'00'

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 MDA Industrial Security

SECURITY GUIDANCE (BLOCK 13) CONTINUATION PAGES:

Special Instructions:

Reporting Requirements:

The Contractor shall provide the following to the MDA Industrial Security Office (contact information listed in block 13 of page two of the DD Form 254):

- Courtesy copy the MDA Industrial Security Office on any security incident report (initial and final) involving the loss, compromise, or suspected compromise of classified information sent to the Defense Security Service. The Contractor shall provide a copy to the MDA within the same reporting timeframe as is required by the Defense Security Service
- Courtesy copy the MDA Industrial Security Office on any report involving a cyber-intrusion of MDA program information sent to the Federal Bureau of Investigation and the Defense Security Service per NISPOM Chapter 1, Section 301 and Industrial Security Letter 2013-05.
- Provide a copy of any Defense Security Service letter that indicates a less than satisfactory security rating and/or that negatively impacts the Facility Clearance Level (FCL) of the company within 48-hours of receipt.
- Provide electronic copies of Subcontractor DD Form 254s issued by the Prime and the Subcontractor. The Prime Contractor shall act as the focal point for collecting their Subcontractor's DD Form 254s and the Prime is responsible for forwarding these DD Form 254s to the MDA Industrial Security Office.

In accordance with NISPOM Chapter 1, Section 300, the Contractor and its subcontractors shall notify the Contracting Officer, the Contracting Officer's Representative, and MDA Industrial Security in writing within 24 hours of becoming aware of adverse information regarding an employee, who works within a Government/MDA facility, which could affect their access to classified information. Reportable information is described in DoD Regulation 5200.2-R, paragraph C2.2.1. and Appendix 8.

Subcontractor Classified Access Approvals:

The Prime Contractor and Subcontractor are authorized to flow access to and/or dissemination of classified information to the TOP SECRET level to their Subcontractor. Dissemination is only authorized and applicable for information safeguarded at the Contractor's facility. This authorization includes access to Non-Sensitive Compartmented Information (SCI) (NISPOM Chapter 9, Section 304), Communications Security (COMSEC) (NISPOM Chapter 9, Section 407), Critical Nuclear Weapon Design Information (CNWDI) (NISPOM Chapter 9, Section 204), and North Atlantic Treaty Organization (NATO) (NISPOM Chapter 10, Section 708) information. The Contractor shall provide the appropriate accesses to its Subcontractors as required per NISPOM 5-502. The Prime Contractor and Subcontractor must verify Facility Clearance, Safeguarding Capability and Access Authorizations prior to the dissemination of classified information. The following require specific authority: SCI - not authorized to flow without prior approval from MDA/Special Security and Special Access Program (SAP) - not authorized to flow without prior approval from MDA/Special Programs.

Request for Proposals:

This section concerns the release of classified information to the contractor regarding the government's **Request for Proposal**; MDA classified information may only be released to the Contractor for submission preparation purposes following verification of the Contractor's facility clearance and safeguarding. The DD Form 254 shall act as security guidance for the safeguarding of IRES related classified information at the Contractor facility. The Defense Security Service maintains security cognizance of classified information stored at a Contractor facility. However, the following stipulations apply:

- IAW NISPOM paragraphs 5-200 and 5-600, Contractors shall ensure full written accounting and control over all MDA classified information provided to the Contractor by MDA or created as copies by the Contractor.
- IAW NISPOM paragraphs 5-501 and 5-502, distribution of MDA classified information shall only be made to those cleared Contractor personnel working on the Contractor's response to the request for information, unless otherwise authorized by the Program Manager (PM).
- IAW NISPOM paragraph 5-509, for purposes of this submission request, further distribution of MDA classified information shall only be authorized by the MDA PM overseeing this request for information.
- IAW NISPOM paragraphs 5-702, 5-703, and 5-704, all classified information provided for use in submission preparation shall be returned to MDA or destroyed.

Reference Item 8.a. (continued) Government Locations:
Classified performance will occur at various MDA and/or government locations as directed by the contract via the Performance Work Statement, Statement of Work, or Statement of Objectives or other agreement. The Contractor shall abide by the host government security requirements per NISPOM Chapter 1, Section 200 and Chapter 6, Section 105c. The cognizant security office at the performance location is MDA or the host installation.

Reference Item 8.a. (continued) Performance Locations include the following Contractor Facilities:

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE

Per NISPOM Chapter 5 Section 504, the Contractor can disclose classified information between cleared facilities within the Multiple Facility Organization (MFO). MDA does not limit which cleared locations are considered performance locations within the MFO. It is the Contractor's responsibility to comply with Defense Security Service policy and procedures for establishing a classified performance location within the MFO structure. This guidance does not apply to government locations or other Contractor company locations at which the prime Contractor will be conducting classified performance.

Reference Item 10.a and 11.h: The Contractor shall comply with the requirements of NISPOM Chapter 9, Section 4 and National Security Agency/Central Security Service Policy Manual Number 3-16, Control of Communications Security (COMSEC) Material, for access to and safeguarding of COMSEC information.

Reference Item 10.b & d: Contractors shall adhere to the requirements of DoDI 5210.02, "Access to and Dissemination of Restricted Data (RD) and Formerly Restricted Data (FRD)," 3 June 2011, for access and training requirements. **Flow this requirement to subcontractors when applicable.**

1. Contractors shall possess a valid DoD security clearance at a level commensurate with the information concerned and shall have a need-to-know for access. DoD contractors require a final Secret security clearance for access to Secret RD information. Contractors shall have a final Top Secret security clearance for access to Top Secret RD information. NISPOM section 2-211a. applies.

2. The Prime contractor and its subcontractors shall be required to complete training for access to RD/FRD material and for derivative classification of RD/FRD information. This training is provided by the Department of Energy (DOE) and can be accessed at the DOE website (http://energy.gov/hss/services/classification/classification-training-institute/training-other-agency-personnel).

a. For individuals with access to RD/FRD information, personnel shall complete the "Classification of Nuclear Weapons-Related Information (Restricted Data and Formerly Restricted Data)" course. The contractor company shall maintain a record of the training for each individual with access to RD/FRD. These records shall be made readily available during security inspections or for other government purposes. Records shall be maintained for two years after an individual no longer requires access to RD/FRD information.

b. For individuals who will conduct derivative classification, personnel shall complete the "Restricted Data Classifiers Course." Upon completion of the course, the contractor company shall request a written exam from MDA. MDA will grade the written exam and will provide a certificate of completion. The contractor shall at a minimum obtain an 80% to successfully pass the exam. The contractor company shall maintain a record of the training for each individual designated as a RD Classifier. These records shall be made readily available during security inspections or for other government purposes. Records shall be maintained for two years after an individual is no longer designated as a RD Classifier.

3. Contractors should contact the MDA Industrial Security office listed in block 13 of the DD 254 for information and materials concerning the RD Classifier exam.

Reference Item 10.c: NISPOM Chapter 9, Section 2 requirements apply. Access to Critical Nuclear Weapons Design Information requires a final clearance.

Reference Item 10.e.(1): This contract requires access to Sensitive Compartmented Information (SCI) material. The Contractor is not required to have an accredited SCI Facility but requires access to SCI at other locations. Additionally, the Facility Security Officer will ensure that when a Contractor with access to SCI is due for a Periodic Reinvestigation, the Periodic Reinvestigation request is conducted to meet SCI standards. Written U.S. Government approval by MDA/Special Security is required prior to giving SCI access to a Subcontractor. Additional requirements are included in the attached SCI Supplement.

Reference Item 10.e.(2): NISPOM Chapter 9, Section 3 requirements apply.

Reference Item 10.f: Requirements are included in the attached SAP Supplement.

Reference Item 10.g: NISPOM Chapter 10, Section 7 requirements apply.

Reference Item 10.h: NISPOM Chapter 10, Section 3 requirements apply.

Reference Item 10.j: See For Official Use Only/Controlled Unclassified Information (FOUO/CUI) Supplement below. **The Contractor is required to provide the supplement to all uncleared Subcontractors requiring access to FOUO/CUI information.**

Reference Item 11.c: The Contractor has a responsibility to understand and use all applicable Security Classification Guidance (SCG) provided by the government (reference NISPOM 4-102). The MDA has provided a list below of necessary SCGs required to conduct derivative classification. The Contractor shall request the required SCGs from the Contracting Officer's Representative (COR). The MDA has the obligation to review existing guidance periodically during the performance stages of the contract and to issue a revised DD Form 254 when a change to the SCGs occurs or when additional SCGs are needed (reference NISPOM Chapter 4, Section 103b.). The Contractor shall flow-down required SCGs on its Subcontractor DD Form 254s and shall provide copies of the SCGs to its Subcontractor. The following security classification guidance applies:

1. Ballistic Missile Defense System (BMDS) Security Classification Guide (SCG), dated 19 October 2010 to include Admin Changes dated 11 July 2011.
2. Terminal High Altitude Area Defense (THAAD) Security Classification Guide (SCG), dated 29 November 2001, to include Admin Changes dated 29 December 2014.
3. Aegis Ballistic Missile Defense (ABMDS) Security Classification Guide (SCG), Change 1 dated 22 May 2009 to include Admin Changes dated 11 July 2011.
4. Defense Support Program (DSP) Space Based Infrared System (SBIRS) Highly Elliptical Orbit (HEO) Operations Security Classification Guide (SCG), dated 01 October 2009.

5. OPNAVINST 5513.3C, Standard Missile-2/3/4/6 Security Classification Guide (SCG), dated 01 October 2012.
6. Space Tracking & Surveillance System Demonstrator Satellite (STSS) Security Classification Guide (SCG), dated 12 September 2007 to include Change 2 dated 15 October 2011.
7. STRATCOM Integrated Missile Defense (IMD) Security Classification Guide (SCG), dated 01 January 2015.
8. Ground-Based Midcourse Defense (GMD) Security Classification Guide (SCG), dated 07 August 2006 to include Admin Changes dated 11 July 2011.
9. Joint United States (US)-Government of Israel (GOI) Arrow System Improvement Program (ASIP) Security Instructions and Classification Guide (SCG), dated 01 July 2004 to include Admin Changes 11 July 2011.
10. Airborne Laser Program Group (ABL) Security Classification Guide (SCG), dated 27 May 2003, to include Admin Changes dated 22 August 2011.
11. U.S. Air Force Intercontinental Ballistic Missile (ICBM) Security Classification/Declassification Guide (SCG), dated 23 October 2008.
12. Ballistic Missile Defense (BMD) Radars Security Classification Guide (SCG), dated 22 July 2013.
13. Other Security Classification Guides will be provided as required.

Reference Item 11.d: The Contractor is required to provide adequate storage and transportation for classified hardware to the level of TOP SECRET. If the classified hardware is of such a size or quantity that it cannot be safeguarded in a regular-sized GSA-approved storage container, a Closed Area, Vault, or additional security containers may be required. Per the NISPOM, the Defense Security Service has responsibility for the authorization and approval of all Closed Areas and/or Vaults within the Contractor's facility.

Reference Item 11.f:

1. The Contractor shall require access to classified information overseas at areas designated in the Statement of Work, Performance Work Statement, or Statement of Objectives.

2. All Contractor personnel working at the designated location(s) and accessing classified information shall obtain an Area of Responsibility-specific travel briefing and Antiterrorism Level I Awareness training prior to departing on travel. Required training shall be received within 90 days prior to travel.

3. The Contractor shall submit foreign visit requests as dictated by the NISPOM, Chapter 10, Section 5. A Contractor shall submit the visit request through the Defense Security Service-designated security official.

4. The Contractor is not authorized per the NISPOM to establish a contractor facility outside of the U.S., its possessions, or its territories. Storage, custody, and control of classified information required by a U.S. Contractor employee abroad is the responsibility of the U.S. Government. Storage of classified information shall be at a U.S. military facility, a U.S. Embassy or Consulate, or another location occupied by a U.S. Government organization.

Reference Item 11.g: The Contractor is authorized to use the services of the Defense Technical Information Center (DTIC) or other secondary distribution center. As required, the Contractor will prepare and submit the DD Form 1540, "Registration for Scientific and Technical Information Services" and DD Form 2345, "Militarily Critical Technical Data Agreement" to the contracting office for approval. Subcontractors are required to submit requests through the Prime Contractor.

Reference Item 11.j: The Contractor is required to apply Operations Security (OPSEC) to enhance protection of classified and unclassified critical information pursuant to DoD Directive 5205.02, "DoD OPSEC Program; DoD 5205.02-M, "OPSEC Program Manual;" National Security Decision Directive Number 298, "National Operations Security Program;" MDA Instruction 5205.02, "OPSEC Program;" and supplementary instructions. Service OPSEC guidance may also apply if the contracted activity is performed in a Service-level operational environment. If a conflict is identified between Service and higher-level guidance, contact the MDA OPSEC Staff for clarification.

Reference Item 11.l:

Contractor's Unclassified Automated Information System (AIS):

1. The Contractor shall safeguard and protect CUI provided by or generated for the Government (other than public information) that transits or resides on any non-Government information technology system IAW the procedures in DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012, Enclosure 3. Information shall be protected from unauthorized access, disclosure, incident or compromise by extending the safeguarding requirements and procedures in DFARS clause 252.204-7012, Safeguarding of Unclassified Controlled Technical Information. The NIST 800-53 security controls specified in 252.204-7012 shall be extended to include Controlled Unclassified Information (CUI) information which resides on, or transits through the contractor's (prime and all sub-contractors) unclassified information technology systems.

2. The contractor shall ensure that all persons accessing CUI, which includes FOUO, meet the qualifications for an Automated Data Processing/Information Technology (ADP/IT)-III Position requirement).

3. The "For Official Use Only/Controlled Unclassified Information Supplement" provides additional guidance for the handling, marking, transmission, reproduction, safeguarding, and disposition of FOUO/CUI.

4. MDA-reserves the right to conduct compliance inspections of Contractor unclassified information systems and other repositories for the protection of FOUO/CUI.

Reference Item 12: The Prime Contractor shall forward all requests for public release authorization through the Contracting Officer's Representative to the listed MDA program office. Per NISPOM section 5-511, the Contractor shall include all necessary information to assist with the decision of the MDA program office. Per NISPOM Chapter 7, Section 102c., the Prime Contractor shall act as the focal point for all Subcontractor requests for public release. A lack of response from the MDA program office does not constitute as public release authorization. The Prime Contractor shall not release information to the public prior to receiving written authorization from the MDA program office (this requirement includes any information system that provides public access).

Reference Item 14: Program Protection is required for this contract. The interdisciplinary requirements associated with Program Protection are further addressed in Sections C & J of this contract and detailed in the Government issued Program Protection Plan (PPP). The contractor shall implement applicable security countermeasures to protect classified and/or unclassified Critical Program Information and Critical Components as outlined in the Statement of Work/Performance Work Statement/Statement of Objectives and refined in the PPP.

FOR OFFICIAL USE ONLY/CONTROLLED UNCLASSIFIED INFORMATION SUPPLEMENT

1. Definitions.

a. Controlled Unclassified Information (CUI). Unclassified information which requires access and distribution limitations prior to appropriate coordination and an official determination by cognizant authority approving clearance of the information for release to one or more foreign governments or international organizations, or for official public release. Per DoD Manual 5200.01, Volume 4 it includes the following types of information: "For Official Use Only" (FOUO); "Sensitive But Unclassified" (State Department information); "DEA Sensitive Information" (Drug Enforcement Agency information); "DoD Unclassified Controlled Nuclear Information"; "Sensitive Information" as defined in the Computer Security Act of 1987; and information contained in technical documents (i.e., Technical Data) as discussed in DoD 5230.24, 5230.25, International Traffic in Arms Regulation (ITAR), and the Export Administration Regulations (EAR).

b. Dual Citizenship. A dual citizen is a citizen of two nations. For the purposes of this document, an individual must have taken an action to obtain or retain dual citizenship. Citizenship gained as a result of birth to non-U.S. parents or by birth in a foreign country to U.S. parents thus entitling the individual to become a citizen of another nation does not meet the criteria of this document unless the individual has taken action to claim and to retain such citizenship.

c. For Official Use Only (FOUO). FOUO is a dissemination control applied by the DoD to unclassified information that may be withheld from public disclosure under one or more of the nine exemptions of the Freedom of Information Act (FOIA) (See DOD 5400.7-R). FOUO is not a form of classification to protect U.S. national security interests.

d. National of the United States.Title 8, U.S.C. Section 1101(a)(22), defines a National of the U.S. as:

(1) A citizen of the United States, or,

(2) A person who, but not a citizen of the U.S., owes permanent allegiance to the U.S.

NOTE: 8 U.S.C. Section 1401, paragraphs (a) through (g), lists categories of persons born in and outside the U.S. or its possessions that may qualify as Nationals and Citizens of the U.S. This subsection should be consulted when doubt exists as to whether or not a person can qualify as a National of the U.S.

e. U.S. Person. Any form of business enterprise or entity organized, chartered, or incorporated under the laws of the United States or its possessions and trust territories and any person who is a citizen or national (see National of the United States) of the United States, or permanent resident of the United States under the Immigration and Nationality Act.

2. Access.

a. Access to FOUO/CUI must be limited to U.S. Persons that have a current U.S. security clearance (minimum interim SECRET clearance); or have been the subject of a favorably completed National Agency Check with Inquiries (NACI) or a more stringent personnel security investigation. Access approval by MDA/Special Security is pending completion of a favorable NACI or Contractor equivalent.

(1) Contractor Equivalent: Contractor equivalent includes various background checks such as those performed by employers during hiring process. Minimum checks shall include Citizenship, Personal Identification (Social Security Number), Criminal, and Credit. Contractors shall submit a request for approval on company letter head to MDA/Special Security.

(2) Contractor personnel with dual citizenship that have an active U.S. security clearance (interim Secret or higher) can have access to FOUO/CUI material.

(3) Contractor personnel with dual citizenship that do not have an active U.S. security clearance (interim Secret or higher), the following actions will be completed prior to authorizing access to FOUO/CUI material:

(a) The dual citizen shall surrender the foreign passport to the security office

(b) The Contractor Company shall provide a signed letter to the dual citizen informing them that if they request their passport be returned to them, or they obtain a new foreign passport, they will be immediately removed from the MDA program. The dual citizen shall acknowledge by signing and dating the letter.

(c) The MDA Program Manager and MDA/Special Security shall be notified and will provide written approval.

b. Non-Sensitive Positions (ADP/IT-III positions). Non-sensitive positions associated with FOUO/CUI are found at Contractor facilities processing such information on their (Contractor's) unclassified computer systems. Personnel nominated to occupy ADP/IT-III designated positions (applies to any individual that may have access to FOUO/CUI on the Contractor's computer system) must have at least a National Agency Check with Inquiries (NACI) or Contractor equivalent (company hiring practices reviewed and approved by MDA/Special Security). When "Contractor equivalent" option is NOT authorized and there is no record of a valid investigation, the Contractor shall contact MDA/Special Security at mdasso@mda.mil, and provide the requested information. MDA/Special Security will assist the Contractor complete the SF85, Position of Trust Questionnaire, and fingerprints.

3. Identification Markings. FOUO/CUI shall be marked in accordance with DoDM 5200.01, Volume 4, Enclosure 3, Section 2.c.

4. Handling. Storage of FOUO/CUI outside of Contractor facilities (i.e. residence, telework facility, hotel, etc.) shall be in a locked room, drawer, filing cabinet, briefcase, or other storage device. Continuous storage of FOUO/CUI outside of a Contractor facility shall not exceed 30 days unless government approval is granted.

5. Transmission/Dissemination/Reproduction.

a. Subject to compliance with official distribution statements, FOUO markings (e.g., Export Control, Proprietary Data) and/or Non-Disclosure Agreements which may apply to individual items in question; authorized Contractors, consultants and grantees may transmit/disseminate FOUO/CUI information to each other, other DoD Contractors and DoD officials who have a legitimate need to know in connection with any DoD authorized contract, solicitation, program or activity. The government Procuring Contracting Officer (PCO) will confirm with the Contracting Officer's Representative or Task Order Monitor "legitimate need to know" when required. The MDA/Chief Information Officer has determined that encryption of external data transmissions of FOUO/CUI are now practical. The MDA/Chief Information Officer has stated that Public Key Infrastructure (PKI) and Public Key (PK) enabling technologies are available and cost effective. The following general guidelines apply:

(1) In accordance with DoD Manual 5200.01, Volume 4, "Controlled Unclassified Information (CUI)," Enclosure 3, external electronic data transmissions of CUI/FOUO shall be only over secure communications means approved for transmission of such information. Encryption of e-mail to satisfy this requirement shall be in accordance with MDA Directive 8190.01, Electronic Collaboration with Commercial, Educational, and Industrial Partners, May 12, 2009, being accomplished by use of DoD approved Public Key Infrastructure Certification or by the company's participation in the "Federal Bridge."

(2) The MDA/Chief Information Officer (CIO), PKI Common Access Card (CAC) point of Contact is, Ms. Ingrid Weecks (719-721-7040).

b. Failure of the Contractor to encrypt FOUO/CUI introduces significant risks to the BMDS mission. It is essential for the Contractor to understand that mitigation options that are available. The Contractor must understand that failure to encrypt FOUO/CUI carries with it certain risks to the mission. These risks can be mitigated with the thoughtful application of processes, procedures, and technology. Some of the available mitigation tools include:

(1) Approved DoD PKI/CAC hardware token certificates or DoD trusted software certificates for encrypting data in transport.
(2) Industry best practice of Virtual Private Network (VPN) Internet Protocol Security (IPSEC) for intra-organization transport.
(3) Industry best practice of Secure Sockets Layer Portal Web Services for document sharing and storage
(4) Approved DoD standard solutions for encrypting data at rest.
(5) Approved DoD E-Collaboration services via MDA Portal or Defense Information Systems Agency (DISA) Network Centric Enterprise Services (NCES).

(6) Any FIPS 140-2 validated encryption [e.g., IPSEC, Secure Socket Layer/Transport Layer Security (SSL/TLS), Secure/Multipurpose Internet Mail Extension (S/MIME).
(7) Procure and employ Secure Telephone Equipment (STE).
(8) Procure and employ secure facsimile (FAX) capability.
(9) Utilize secure VTC capabilities.
(10) Hand-carry FOUO/CUI.
(11) Utilize mailing through U.S. Postal Service.
(12) Utilize overnight express mail services.

c. FOUO/CUI shall be processed and stored internally on Automated Information Systems (AIS) or networks 1) when distribution is to an authorized recipient and 2) if the receiving system is protected by either physical isolation or a password protection system. Holders shall not use general, broadcast, or universal e-mail addresses to distribute FOUO/CUI. Discretionary access control measures may be used to preclude access to FOUO/CUI files by users who are authorized system users, but who are not authorized access to FOUO/CUI. External transmission of FOUO/CUI shall be secured using NIST-validated encryption. FOUO/CUI cannot be placed on any publically-accessible medium.

d. Reproduction of FOUO/CUI may be accomplished on unclassified copiers within designated government or Contractor reproduction areas.

6. Storage. During working hours, reasonable steps shall be taken to minimize the risk of access by unauthorized personnel (e.g., not reading, discussing, or leaving FOUO/CUI information unattended where unauthorized personnel are present). After working hours, FOUO/CUI information may be stored in unlocked containers, desks, or cabinets if contract building security is provided. If such building security is not provided or is deemed inadequate, the information shall be stored in locked desks, file cabinets, bookcases, locked rooms, etc.

7. Disposition.

a. When no longer required, FOUO/CUI shall be returned to the MDA office that provided the information or destroyed by any of the means approved for the destruction of classified information or by any other means that would make it difficult to recognize or reconstruct the information.

b. Removal of the FOUO/CUI status can only be accomplished by the government originator. The MDA COR shall review and/or coordinate with proper authority the removal of FOUO/CUI status for information in support of contract activity.

Special Access Program (SAP) Supplement

Contract No: H95001-15-R-0001

March 21, 2014 Version—all other versions obsolete.

1. Item 10f:

a. This contract involves DoD SAPs. Strict requirements for need-to-know, special handling, physical security measures, and administrative controls beyond the requirements of the National Industrial Security Program (NISP) are required. SAP participants must comply with the enhanced security procedures outlined in this document.

b. Access to MDA SAP information or material is authorized only at facilities and locations specifically approved by MDA Special Programs. Access to SAP information requires a final U.S. Government TOP SECRET clearance with a favorable NACLC, PRS, SSBI, PPR, or periodic reinvestigation, as appropriate, completed within the last five (5) years, an approved SAP nomination, and a signed special access non-disclosure agreement prior to access. The government program security officer (PSO) will contact the contractor facility security officer (FSO) to obtain security information on facilities and personnel required to perform on this contract.

c. All SAP work, regardless if in a prime or subcontractor's location, will be performed in an MDA-approved SAP facility (SAPF). If there is a requirement to discuss, store, or process SAP information in an existing sensitive compartmented information facility (SCIF), SAPF, or closed area, a memorandum of understanding (MOU) for co-utilization must be executed between the MDA-cognizant SAP security representative and the other government or contractor customer cognizant security representative. A co-utilization agreement (CUA) is required between MDA Special Programs and the SCI-cognizant security authority (CSA) prior to introduction of MDA-sponsored SAP data into a SCIF. A standard operating procedure (SOP) will be written for each SAPF and coordinated with MDA Special Programs.

2. Item 11h: Consult with MDA Special Programs prior to ordering encryption devices or COMSEC keying material (other than STEs) to support SAP transmissions.

3. Item 11i: TEMPEST requirements may be necessary in the performance of this contract in accordance with program requirements, JAFAN 6/3, and where appropriate, JAFAN 6/0.

4. Item 11j: OPSEC measures are necessary in the performance of this contract. Specific guidance will be provided by MDA Special Programs.

5. Item 12:

a. Public release of SAP information is ***prohibited***. Do not release documents or other materials pertaining to this effort to the Defense Technical Information Center (DTIC) or any other such information service under any circumstance. A pre-publication and/or presentation(s) review is required prior to the use of any classified or unclassified information which is either tangentially or directly related to any SAP. In each case, approval must be obtained from the MDA SAP Central Office (SAPCO). The request must be submitted by the person who desires

to make the publication or presentation, via the contractor program security officer (CPSO) to the MDA government program security officer.

b. The contractor shall not use references to SAP accesses (nicknames, code words, et. al) or information, even by unclassified acronyms, in advertising, promotional efforts, or employee recruitment.

6. Item 13: The Government PSO will provide additional security classification guides (SCG) specific to the SAPs under this contract. Contractors will classify SAP material in accordance with the provided SCGs and applicable publications listed in Item 14.

a. Prior to processing, storing, transmitting, transferring, or communicating MDA SAP information on any IS or network, the contractor shall comply with certification and accreditation controlling laws, regulations, DoD and MDA SAPCO policy as referenced in Item 14 and be required to obtain the requisite accreditation to test or operate from the MDA SAPCO Designated Accrediting Authority (DAA).

b. The Contractor shall employ physical security safeguards for IS(s) and/or networks involved in processing or storage of Government information/data to prevent unauthorized access, disclosure, modification, destruction, use, and to otherwise protect the confidentiality and ensure use conforms with DoD regulations.

7. Item 14: Contractors performing under this contract will use the below listed security publications unless exempted by MDA Special Programs. MDA Special Programs will provide the contractor the below listed publications if the contractor does not have prior access to them.

a. JAFAN 6/0, Revision 1, "Special Access Program Security Manual."
b. DoD Joint Special Access Program (SAP) Implementation Guide (JSIG), October 9, 2013
c. DoD Memo, "Transition to the Risk Management Framework," December 18, 2013
d. The MDA Special Programs "SAP Nomination Process (SAPNP)."
e. JAFAN 6/9, "Physical Security Standards for SAP Facilities."
f. DoD 5220.22M Sup 1, "National Industrial Security Program Operating Manual Supplement; DoD Overprint to the NISPOMSUP."
g. Applicable PSO-approved facility-specific SOPs, treaty plans, and OPSEC guides.
h. DoD Directive 5205.07, "Special Access Program (SAP) Policy."
i. DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)."
j. MDA SAPCO Policy, "Certification and Accreditation Program."
k. National Security Agency/Central Security Service (NSA/CSS) Policy Manual 9-12.
l. MDA Special Programs, "Top Secret Control Officer's (TSCO's) Guide."
m. DoD Manual 5205.07, Volume 4, "Special Access Program (SAP) Security Manual: Marking."
n. DoD "Security Marking Implementation Guide for Special Access Programs."
o. JAFAN 6/3, Protecting Special Access Program Information Within Information Systems, and JAFAN 6/3 Implementation Guide.

8. Item 15: MDA Special Programs will conduct program/security reviews of all SAPFs, material, and operations related to this contract. DSS oversight over SAP portions of this contract is carved-out.

9. Contract Number. The contractor may be required to establish non-attributable, internal procedures and charge numbers that will be documented in their business financial management procedures as necessary for cost accumulation by uncleared personnel.

10. Subcontracting. Subcontracting must have prior approval from MDA Special Programs. Any classified program activity requiring the use of a subcontractor facility must meet JAFAN 6/9 criteria and be approved by MDA Special Programs.

11. Communications and Transmissions.

a. All material relating to this contract and its administration shall be classified in accordance with MDA and SAP-specific SCGs and this DD Form 254, or as directed by MDA Special Programs.

b. Program-related communications will be conducted on secure communication devices.

12. Vouchers. All invoices submitted under this contract shall be ***unclassified*** and shall remain devoid of any information requiring them to be classified or cause an OPSEC concern. The invoice/voucher ***may not*** reveal the contractor's name, customer's name, ***and*** any funding figures.

13. Legal Counsel. Notify the PCO and MDA Special Programs, in writing, should the contractor require private counsel to represent corporate interests in matters related to or associated with SAP-sponsored activities. The private counsel shall be treated as a subcontractor. In those incidents where the issues are not program-specific, it is the responsibility of appropriately-indoctrinated contractor personnel to prevent inadvertent disclosure of SAP-related information, operational procedures, and/or administrative details.

14. Retention of Program Related Documentation, Software, and Hardware. Upon completion of this contract and acceptance by the government of final deliverables, the contractor shall:

a. Conduct an inventory/audit of all SAP material received and/or generated under this contract and forward it to MDA Special Programs.

b. In accordance with MDA Special Programs direction, the contractor shall destroy administrative security records and related documents using an approved destruction procedure/method and maintain certificates of destruction for final close-out review. Retention of SAP information at the contractor facility is not generally authorized beyond contract close-out unless a follow-on contract or task is anticipated. A written request for authorization for document retention must be forwarded to the PCO and MDA PSO for approval.

15. Issues/Conflict Reporting.

a. Any questions regarding classification, access, or any other security-related issue in regard to the SAP portion of this contract must be referred to MDA Special Programs.

b. Any conflict between instructions contained in Item 14 and this DD Form 254 must be reported to MDA Special Programs by the most expedient and secure means available.

COR/TM/CLIN COTR Missile Defense Agency	Special Access Program Representative Missile Defense Agency

MDA SCI Supplement (Item 10.e (1)) for DD Form 254

This supplement applies to Prime Contract Number: **H95001-15-R-0001**

Delivery/Task Order Number: _____. Expiration date: _____

A. The following controls will apply to SCI provided under this contract:

1. DoD 5105.21, "Sensitive Compartmented Information Administrative Manual;" ICD 503, "Intelligence Community Information Technology Systems Security Rick Management, Certification and Accreditation;" ICD 704, ICPG 704-1 – 704-5, "Personnel Security Standards and Procedures Governing Eligibility for access to SCI;" ICD 705, ICS 705-1 – 705-2, "Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities;" DoDM 5200.01, "DoD Information Security Program;" and MDA SCI Manual provide the necessary guidance for physical, personnel, and information security measures, to include proper marking requirements, and is part of the SCI security specifications for the contract. NOTE: CSO or FSO are required to process all SCI administration requirements for all MDA SCI contract efforts per the MDA SCI Manual. The Manual can be obtained by contacting MDA Special Security.

2. Inquiries pertaining to classification guidance will be directed to the responsible MDA Contracting Officer's Representative (COR). The name/phone number for the MDA COR is: _____.

(Additionally, identify the Company Security POC (FSO/CSO) & phone number and email address at the contractor's/subcontractor's location): _____.

3. All SCI furnished to the contractor in support of this contract/delivery/task order remains the property of the Department of Defense, or the agency or command that releases it. Upon completion of the contract, SCI furnished to the prime contractor will be returned to MDA or destroyed as directed by the MDA COR. NOTE: Prime contractor and subcontractor company security officers who destroy derivative or MDA generated SCI material will be required to provide a copy of the destruction certificate to the MDA COR.

4. It is the Prime Contractor's responsibility to ensure that all Sub-contractors requesting access to SCI have been properly cleared in accordance with the National Industrial Security Program. The Prime Contractor will provide this SCI Supplement to their Sub-contractors as necessary according to the Sub-contractor's clearance requirements. The Prime Contractor is further advised that SCI Billets used by the Sub-contractor will be subtracted from the total authorized billets allocated for this contract in paragraph 5 below. The COR, the Prime Contractor FSO, and the Sub-contractor FSO will sign SCI nomination requests. A continuing access memo for all current support to the contract must be completed annually and submitted to the MDA SSCO.

5. The contract/delivery/task order requires the following SCI access(es): (COR is required to mark with an "X" the SCI accesses needed to effectively fulfill the SCI contractual obligation) **SI _X_, TK _X_, G _X_, HCS _X_**. Access will be granted by the government agency. Upon completion or cancellation of the contract the MDA COR will provide a by name list of all contractors required to be debriefed from SCI to the MDA SSCO before contract close-out. All debriefed contractors will be removed from MDA SCI billets immediately by the SSCO. Based on mission requirements, this contract may authorize up to **175** SCI billets.

6. Contractor personnel requiring access to SCI and justification for MDA SCI billets will be initiated by the company's security officer with validation by the COR per the guidelines in the MDA SCI Manual. The CSO/FSO should only submit contractors employees who have a completed in scope (within the last 5 years) Single Scope Background Investigation (SSBI) for SCI access. Company Security Officers should submit a SCI Nomination Package (Nom Memo, updated SF86 questionnaire and copy of DD Form 254 (Prime & Sub, as required) to the MDA Special Security Contact Office for processing. Submit only personnel that have a real day-to-day need-to-know requirement. NOTE: The MDA SSCO will not accept SF86 questionnaires dated prior to the 2010 version.

7. The CSO/FSO shall advise the MDA SSCO, through the contracting officer's representative, upon reassignment of personnel to other duties not associated with this contract. NOTE: Individual contractors who no longer support a MDA SCI contract will be debriefed from SCI access immediately. Company security officers are required to coordinate with the MDA SSCO to get their individual contractors debriefed.

8. The CSO must coordinate with the MDA COR prior to subcontracting any portion of the SCI efforts involved in their MDA SCI prime contract. A separate DD Form 254, utilizing this SCI Supplement, for the subcontractor will be processed and a copy provided to MDA SSCO. NOTE: The SSCO will not provide any SCI administration support to prime contractors or subcontractors who do not have a signed active DD 254 for an MDA SCI contract.

9. The contractor shall not use references to SCI accesses, even by unclassified acronyms, in advertising, promotional efforts, or recruitment of employees.

10. All SCI work will be performed in a DIA accredited MDA SCIF unless otherwise authorized. Is there a SCIF required at the Contractor's Facility? _____ Yes or **_X_** No (COR required to mark and "X" in the appropriate space).

11. AIS SCI Processing. Electronic processing of SCI requires accreditation of the equipment in accordance with ICD 503 and DIAM 50-4.

12. Visit Cert. The contractor FSO/CSO will submit the request for SCI visit certifications per guidelines of the MDA SCI Manual through the COR for approval of the visit. The certification request must arrive at MDA Special Security at least five (5) working days prior to the visit.

13. The contractor will not reproduce any SCI related material without prior written permission of the COR.

14. MDA has exclusive security oversight for all SCI released to the contractor or developed under this contract. Defense Intelligence Agency (DIA) is the cognizant security authority for inspections of MDA-sponsored contractor SCIFs to ensure compliance of SCI Directives and Regulations. MDA Special Security will conduct self-inspections of MDA-sponsored SCIFs.

B. The Missile Defense Agency is designated as the User Agency for SCI requirements.

MDA SSCO: Dave Gmaz, Special and Personnel Security

MDA SSCO Signature: _____

Phone: (571) 231-8459

COR/TM/COTR/Directorate designation: _____

COR/TM/COTR Signature: _____

Phone: _____

Directorate Technical Oversight Representative: _____

DTOR Signature: _____

Phone: _____