DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD National Industrial Security Program Operating Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: Secret

b. LEVEL OF SAFEGUARDING REQUIRED: None

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*			**3. THIS SPECIFICATION IS:** *(X and complete as applicable)*			
	a. PRIME CONTRACT NUMBER		X	a. ORIGINAL *(Complete date in all cases)*		DATE *(YYYYMMDD)* 20140604
	b. SUBCONTRACT NUMBER			b. REVISED *(Supersedes all previous specs)*	Revision No.	DATE *(YYYYMMDD)*
X	c. SOLICITATION OR OTHER NUMBER W56HZV-14-R-0031	DUE DATE *(YYYYMMDD)* 20140831		c. FINAL *(Complete item 5 in all cases)*		DATE *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? _____ YES ___X___ 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 254? _____ YES ___X___ 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)
TBD	TBD	TBD

7. SUBCONTRACTOR

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

8. ACTUAL PERFORMANCE

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)
Various RS JPO government locations See Block 13 for sites	N/A	N/A

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

The Robotics, Maintenance, Logistics and Systems Engineering & Technical Assistance (SETA) contractor shall provide program Engineering and Technical Management support, Logistics support, Product Assurance, Test, and Configuration Management (PATCM) support, and Program Management and Administrative Support.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	**11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:**	YES	NO
a. COMMUNICATION SECURITY (COMSEC) INFORMATION		X	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	X	
b. RESTRICTED DATA		X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		X
d. FORMERLY RESTRICTED DATA		X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY		X
(1) Sensitive Compartmented Information (SCI)		X	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
(2) Non-SCI		X	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	X	
f. SPECIAL ACCESS INFORMATION		X	h. REQUIRE A COMSEC ACCOUNT		X
g. NATO INFORMATION		X	i. HAVE TEMPEST REQUIREMENTS		X
h. FOREIGN GOVERNMENT INFORMATION		X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X	
i. LIMITED DISSEMINATION INFORMATION		X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER *(Specify)* Follow and Implement: (1) Threat Awareness and Reporting Requirements (2) Security Training (3) Information Systems Processing Requirements	X	
k. OTHER *(Specify)* (1) Controlled Unclassified Information (CUI) (2) Security Classification Guidance (3) SIPRNET	X				

DD Form 254, DEC 99 *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 National Industrial Security Program Operating 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):*

o PEO CS&CSS, ATTN: SFAE-CSS; Mail Stop 332, ATTN: Public Release Office, 6501 E. 11 Mile Road, Warren, MI 48397-5000, who will obtain public release approval through the prescribed channels to include the PCO and PAO.

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 classified 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.)*

Block 8 Cont'd: Performance Locations: Warren, MI; Selfridge Air National Guard Base, MI; Huntsville, AL; Fort Irwin, CA; 29 Palms, CA; Fort Carson, CO; Tyndall AFB, FL; Fort Benning, GA; Fort Stewart, GA; Fort Riley, KS; Fort Campbell, KY; Fort Polk. LA; Fort Leonard Wood, MO; Camp Shelby, MS; Fort Bragg, NC; Fort Drum, NY; Fort Sill, OK; Fort Bliss, TX; Fort Hood, TX; Fort Lee, VA; Quantico, VA; Fort Eustis, VA; Fort A.P. Hill, VA; Fort Lewis, WA; National Capital Region, Wash. DC

Estimated Completion Date: 9 January 2016

Collateral classified information generated in support of this contract shall be classified in accordance with the source material used or the Security Classification Guide and protected in accordance with the National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22-M, and this DD Form 254. Unclassified information shall be protected IAW the Security Classification Guide, the OPSEC Plan, and Attachment A.

All classified material shall be transmitted IAW the NISPOM (Registered US Mail, cleared commercial carrier (Monday thru Thursday), Same Day Delivery, or secure fax).

Access to technical data by foreign interests is prohibited unless authorized by a valid export authorization.

The following attachments are made part of this DD Form 254:
Attachment A – Guidelines for the Controlled Unclassified Information (Item 10.k., includes Item 10.j (1))

CUI and OPSEC requirements shall be flowed down to all U.S. subcontractors (including unclassified U.S. subcontractors) as an integral part of their respective contracts.

See Continuation of Block 13

"The COR has reviewed this Security Specification and certifies the requirements are complete and adequate for performance of the contract. The COR understands the provisions and will ensure that it is complied with within the limits of his/her responsibility, and that any violations are brought to the attention of the Contracting Officer."

LEWIS.JAMES.W.1244564700
Digitally signed by LEWIS.JAMES.W.1244564700
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=LEWIS.JAMES.W.1244564700
Date: 2014.06.05 08:04:47 -04'00'

James Lewis
Government Contracting Officer Representative

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to NISPOM 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 ☐

Also see Block 13 for additional requirements.

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 item13 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 contract effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
Nancy Chaplin	Senior Security Officer	586-282-9648

d. ADDRESS *(Include Zip Code)*
PEO GCS CIO
SFAE-GCS-CIO/MS 505
6501 East Eleven Mile Road
Warren, MI 48397-5000

e. SIGNATURE
CHAPLIN.NANCY.A.1230490259
Digitally signed by CHAPLIN.NANCY.A.1230490259
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=CHAPLIN.NANCY.A.1230490259
Date: 2014.06.04 14:35:58 -04'00'

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. ADMINSTRATIVE CONTRACTING OFFICER
- ☐ f. OTHERS AS NECESSARY

DD Form 254 Reverse, DEC 99

CONTINUATION OF BLOCK 13 OF THE DD FORM 254

Item 10.j – FOR OFFICIAL USE ONLY (FOUO): FOUO Information generated and/or provided under this contract shall be safeguarded and marked as specified in additional Guidelines for Controlled Unclassified Information (CUI) (Attachment A).

Item 10.k.(1) – CONTROLLED UNCLASSIFIED INFORMATION (CUI) generated and/or provided under this contract shall be safeguarded and marked as specified in additional Guidelines for Controlled Unclassified Information (CUI) (Attachment A).

Item 10.k.(2) – Security Classification Guidance: Unmanned Ground Vehicles Security Classification Guide, dated 12 Sep 2011.

Item 10.k.(3) – SECRET INTERNET PROTOCOL NETWORK (SIPRNET) ACCESS REQUIRED: The contractors granted SIPRNET access shall not access, download or further disseminate any special access data (i.e., intelligence, NATO, COMSEC, etc) without the guidance and written permission of the Government Contracting Officer. Contractors must also be aware that NATO classified material may reside on the SIPRNET and they are not authorized to access, download, or to disseminate any NATO or other special access data (i.e. intelligence, COMSEC, etc.). All contractors shall read the brief entitled NATO Security Briefing Forward found under the forms tab at: https://secureweb.hqda.pentagon.mil/cusr/forms.aspx prior to being issued a SIPRNET account. This briefing does not authorize NATO access, and is solely for the purpose of awareness.

Item 11.a – HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT FACILITY: Contractor performance is restricted to location identified in Block 8a. The performance location shall provide security classification guidance for this contract. Submit visit request through the Government Contracting Officer and/or Security Management Office for need-to-know verification.

Item 11.g – BE AUTHORIZED TO USE THE SERVICES OF THE DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER: The contractor shall prepare DD Forms 1540 and/or 2345 for authorized access to DTIC. Completed forms shall be provided to the Government Contracting Officer to verify the need-to-know and submit the DD forms on behalf of the contractor. Refer to NISPOM Chapter 11, Section 2 for more information.

Item 11.j – OPERATIONS SECURITY (OPSEC) REQUIREMENTS: The contractor shall follow the RS JPO OPSEC Plan, dated 28 October 2013, as well as annexes and updates. The contractor is not required to develop their own OPSEC Plan. To ensure awareness of the RS JPO OPSEC Plan, the contractor shall participate in Government provided annual training for all RS JPO personnel on the contents of the RS JPO OPSEC Plan. New personnel shall receive RS JPO OPSEC Plan specific training provided by the Government within 30 days of program assignment.

Item 11.l.(1) – THREAT AWARENESS AND REPORTING REQUIREMENTS: ICW NISPOM 1-301, the contractor shall report threat-related incidents, behavioral indicators, and other matters of counterintelligence (CI) interest specified in AR 381-12, Chapter 3, through the facility security officer to the government security officer, the nearest military CI office, the Federal Bureau of Investigation, and the Defense Security Service. Annually, train personnel who handle classified information IAW AR 381-12, Chapter 2. This requirement shall be flowed down to all U.S. subcontractors that have access to classified information/material.

Item 11.l.(2) – SECURITY TRAINING: Compliance with and participation in government provided security training is required for the contractor employees whose place of performance is on a government installation.

Item 11.l.(3) – INFORMATION SYSTEMS PROCESSING REQUIREMENTS: For access to Government Information Systems (IS) or systems processing US Government information will be IAW AR 25-2. Contractor employees who require access to government Information Technology (IT) in support of this contract shall be assessed for trustworthiness by a designed Government official prior to granting IT access in accordance with AR 25-2 and AR 380-67. Minimum background investigation requirement for access to Government information systems will be determined IAW AR 25-2. Trustworthiness determinations will be processed IAW DoD 5200.02-R, AR 25-2, and AR 380-67. Contractors who require access to a DA network must be processed in the Contractor Verification System database for a common access card (CAC).

Item 12 – PUBLIC RELEASE: An electronic copy of the request with full text and graphics must be provided through the Government Contracting Officer at least forty-five (45) working days prior to the requested release date. If all or part of the information was generated by another organization, their written release authorization must accompany the request.

Notification of loss or compromise of collateral classified information shall be provided to the Government Program Security Office within 72 hours of the incident, in addition to the reporting requirements outlined in the NISPOM.

ATTACHMENT A

ADDITIONAL GUIDELINES FOR CONTROLLED UNCLASSIFIED INFORMATION

General: There are types of information that are not classified but that require application of access and distribution controls and protective measures for a variety of reasons. This information is known as "controlled unclassified information (CUI)." The types of information considered CUI for the program are information marked "For Official Use Only" by the U.S. Government and technical data. When handling CUI material, all personnel are to comply with these requirements and follow their company policy and/or applicable Proprietary Information Agreements (PIA) concerning the protection of proprietary information in situations not clearly stated herein.

Technical Data Description: Any recorded information related to experimental, developmental, or engineering works that can be used to define an engineering or manufacturing process, or can be used to design, procure, produce, support, maintain, operate, repair, or overhaul program material. The data may be graphic or pictorial delineations in media (e.g., computer software, drawings, or photographs), text in specifications, related performance or design documents, or computer printouts. Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, catalog-item identifications, and related information, and computer software documentation.

For Official Use Only (FOUO) Information Description: "For Official Use Only (FOUO)" is a Government designation applied to **unclassified** information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). FOUO information includes information identified as such in the Security Classification Guide or information from a government document marked FOUO.

CUI Markings

Marking of FOUO documents will be in accordance with Army Regulation (AR) 25-55. Information extracted from an FOUO document will carry the FOUO marking until formally reviewed by the government.
AR 25-55 can be found at http://www.apd.army.mil/pdffiles/r25_55.pdf.

Marking of Technical Data will include the statement provided in the Security Classification Guide. If the contents of the technical document require more than one Distribution Statement, apply the most restrictive statement. This does not preclude additional mandated markings as may be required by the contract.

Protection of CUI Information

Access: CUI may be released only to an individual who has a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose. Information in any media format may only be disseminated on a need-to-know basis. The need-to-know restricts the use or dissemination of CUI data to those individuals or organizations with direct affiliation with the given program or project. Further dissemination of such information will be at the discretion of the Government Security Manager. Personnel no longer requiring access to CUI must delete or surrender any in their possession and terminate future access to it.

Storing/Handling: During working hours, take reasonable steps to minimize risk of access to CUI by unauthorized personnel. After working hours, store CUI information in locked desks, file cabinets, bookcases, locked rooms, or similar means. Do not display CUI in public places (e.g., airports, airplanes, restaurants). Computers used to process CUI do not need to be accredited for classified use. Do not process CUI on public computers (e.g., those available for use by the general public in kiosks, hotel business centers) or computers that do not have access control. Personally owned computers are not authorized to process CUI. Mobile devices used to store CUI electronically (e.g., company-issued laptops, personal electronic devices [PED], removable media) must be physically protected and use NIST/NIAP-approved cryptographic products. These are available at http://iase.disa.mil/pki/eca or http://csrc.nist.gov/cryptval/.

Dissemination: CUI printed documents and material may be transmitted through mail channels or hand-carried without formal courier orders. FOUO information may be disseminated to DoD personnel and DoD contractors to conduct official business for the program. If dissemination is required outside of DoD personnel or DoD contractors, contact the Government Security Manager for approval. Technical data will follow the release instructions identified in the Distribution Statement. Use secure communications whenever possible; however, land-line telephones are more secure than cellular telephones and should be used whenever available for discussions involving CUI. Transmit voice and facsimile transmissions only when you have a reasonable assurance that only authorized recipients will have access to the transmission. Digital transmission shall comply with the below:

- All transmission and/or dissemination of CUI identified with a Distribution Statement or marked “FOUO” (i.e., email and file transfers) must use NIST/NIAP-approved cryptographic vendors and algorithms, e.g., DoD-approved Public Key Infrastructure Certification. These are available at http://iase.disa.mil/pki/eca or http://csrc.nist.gov/cryptval/. This encryption requirement includes passcodes to teleconferences or web conferences where there is a reasonable expectation that CUI may be discussed. When encryption is not available, a government collaborative suite (aka Integrated Digital Environment [IDE]) must be used to transmit CUI. Encrypt all wireless external data connections.

- Contractor-hosted collaborative suites may be used for digital transmission and/or dissemination of CUI by personnel not located on a government backbone (e.g., NIPRNET), provided the following conditions apply:

  - Use only NIST/NIAP-approved cryptographic vendors and algorithms. The latest validation lists may be obtained at http://iase.disa.mil/pki/eca or http://csrc.nist.gov/cryptval/.

  - Use an internally hosted service that does not use a third-party collaborative suite service provider.

- All computers containing CUI must be either protected by physical isolation from all personnel without a valid need for the information or protected using NIST/NIAP-approved cryptographic products. Discretionary access control measures must be used to preclude access to CUI by users who are not authorized access to CUI. After working hours, when not in physical possession of the owner, all electronic assets containing CUI must be afforded a reasonable degree of physical protection to prevent theft of program information (e.g., locking up laptops or cable locking them to a stationary base, storing in trunk, or storing out of sight).

- Do not post CUI to web pages that are publicly available or have access limited only by domain/IP restrictions. As permitted by other contract provisions, CUI may be posted to web pages that control access through the use of a DoD approved Public Key Infrastructure Certification and that provide protection via use of secure sockets, or other equivalent technologies. These are available at http://iase.disa.mil/pki/eca.

- As new technologies become available in the electronics arena, care should be given to providing a reasonable degree of protection from known vulnerabilities.

- The Internet is “Public Access”. CUI must be reviewed and officially approved by the PEO GCS Public Affairs Officer for public release before placing on the Internet. This is not applicable when the Internet is used for e-mail transmissions and encryption is used as noted above.

Disposal: Destroy CUI documents by any means approved for the destruction of classified information, i.e. cross-cut shredding or other means that would make it difficult to recognize or reconstruct the information. Clear, purge, or destroy CUI on removable media IAW BBP 03-PE-O-0003 Army Information Assurance Sanitization of Media to AR 25-2. This is available at https://informationassurance.us.army.mil.

Report of Loss of CUI: Report any loss of CUI or loss of CUI from a contractor information system that is known to the contractor within the period of performance of this contract to the Government Security Manager. Initial reports shall be made as expeditiously as possible in all cases within 72 hours of discovery. If additional information is required after submission and review of the initial report, guidance will be provided at that time. Mark any reports For Official Use Only, exemptions 2 and 5 apply. Initial report content shall include the following information as available.

- Applicable dates, including dates of compromise and dates of discovery
- Threat methodology, including all known resources used (e.g. IP addresses, domain names, software tools)
- Account of what actions the threat(s) may have taken on victim system/network
- What information may have been compromised, exfiltrated, or lost, and its potential impact on government programs

Report of Cyber Intrusions: Report cyber intrusions or other compromises of CUI to your supporting counterintelligence office, which will inform the DoD-DIB Common Information Sharing Environment (DCISE). Notify the Government Security Manager of any incidents as well. Refer to Report of Loss of CUI for what needs to be reported, when, and how.