

DEPARTMENT OF DEFENSE

CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(Please read Instructions BEFORE completing this application.) (The requirements of the National Industrial Security Program (NISP) apply to all security aspects of this effort involving classified information.)

OMB No. 0704-0567
OMB approval expires
October 31, 2020

The public reporting burden for this collection of information, 0704-0567, is estimated to average 70 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Washington Headquarters Services, at whs.mc-aies esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

RETURN COMPLETED FORM AS DIRECTED IN THE INSTRUCTIONS.

1. CLEARANCE AND SAFEGUARDING

a. LEVEL OF FACILITY SECURITY CLEARANCE (FCL) REQUIRED
(See instructions.)

TOP SECRET

b. LEVEL OF SAFEGUARDING FOR CLASSIFIED INFORMATION/MATERIAL
REQUIRED AT CONTRACTOR FACILITY

SECRET

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

☒ a. PRIME CONTRACT NUMBER (See instructions.)
H92222-14-C-0026

☐ b. SUBCONTRACT NUMBER
SEE CONTINUATION PAGE

☐ c. SOLICITATION OR OTHER NUMBER DUE DATE (YYYYMMDD)

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

☐ a. ORIGINAL (Complete date in all cases.) DATE (YYYYMMDD)
20140207

☒ b. REVISED (Supersedes all previous specifications) REVISION NO. 5 DATE (YYYYMMDD)
20180621

☐ c. FINAL (Complete Item 5 in all cases.) DATE (YYYYMMDD)

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

In response to the contractor's request dated _____, retention of the classified is authorized for the period of: _____

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

a. NAME, ADDRESS, AND ZIP CODE

Mastodon design LLC
176 Anderson Ave. (b)(7)(F)
Rochester NY 14607

b. CAGE CODE

6ZZG2

c. COGNIZANT SECURITY OFFICE (CSO) (Name, Address, ZIP Code, Telephone)

New York Field Office (IOFNN)
1600 Stewart Avenue (b)(7)(F)
Westbury, NY 11590
(b)(6)

7. SUBCONTRACTOR(S)

a. NAME, ADDRESS, AND ZIP CODE

SEE CONTINUATION PAGE

b. CAGE CODE

c. COGNIZANT SECURITY OFFICE (CSO) (Name, Address, ZIP Code, Telephone)

8. ACTUAL PERFORMANCE

a. LOCATION(S) (For actual performance, see instructions)

SEE CONTINUATION PAGE

b. CAGE CODE

c. COGNIZANT SECURITY OFFICE (CSO) (Name, Address, ZIP Code, Telephone)

9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT

Replacement Joint Threat Warning System (JTWS) GSK in support of U.S. Special Operations Command (USSOCOM).

Period of Performance: 07 FEB 2014 – 22 APR 2019 (Annual DD FM 254 Review Required)

10. CONTRACTOR WILL REQUIRE ACCESS TO: (X all that apply. Provide details in Blocks 13 or 14 as set forth in the instructions.)

☐ a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION

☐ b. RESTRICTED DATA

☐ c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)
(If CNWDI applies, RESTRICTED DATA must also be marked.)

☐ d. FORMERLY RESTRICTED DATA

☐ e. NATIONAL INTELLIGENCE INFORMATION:

(1) Sensitive Compartmented Information (SCI) ☒

(2) Non-SCI ☒

☐ f. SPECIAL ACCESS PROGRAM (SAP) INFORMATION

☐ g. NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION

☐ h. FOREIGN GOVERNMENT INFORMATION

☐ i. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM) INFORMATION

☒ j. CONTROLLED UNCLASSIFIED INFORMATION (CUI) (See instructions.)

☐ k. OTHER (Specify) (See instructions.)

DD FORM 254, NOV 2017

PREVIOUS EDITION IS OBSOLETE.

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL: (X all that apply. Provide details in Blocks 13 or 14 as set forth in the instructions.)

<input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY (Applicable only if there is no access or storage required at contractor facility. See instructions.)	<input type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT
<input type="checkbox"/>	b. RECEIVE AND STORE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT
<input checked="" type="checkbox"/>	c. RECEIVE, STORE, AND GENERATE CLASSIFIED INFORMATION OR MATERIAL	<input type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS
<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	<input type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE (DCS)
<input type="checkbox"/>	e. PERFORM SERVICES ONLY	<input checked="" type="checkbox"/>	l. RECEIVE, STORE, OR GENERATE CONTROLLED UNCLASSIFIED INFORMATION (CUI). (DoD Components: refer to DoDM 5200.01, Volume 4 only for specific CUI protection requirements. Non-DoD Components: see instructions.)
<input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input checked="" type="checkbox"/>	m. OTHER (Specify) (See instructions)
<input type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	SEE CONTINUATION PAGE	

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 (NISPO) or unless it has been approved for public release by the appropriate U.S. Government authority. Proposed public releases shall be submitted for review and approval prior to release to the appropriate government approval authority identified

☐ DIRECT ☒ THROUGH (Specify)

PUBLIC RELEASE AUTHORITY

Requests must be forwarded through the responsible Contracting Official (Item 16), Certifying Official (Item 17) and the HQ USSOCOM Special Operations Communication Office (SOCS-SOCO) prior to public release.

13. SECURITY GUIDANCE. The security classification guidance for classified information 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 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.)

SEE CONTINUATION PAGE

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to NISPO requirements for classified information, are established for this contract.

☒ No ☐ Yes (If Yes, identify the pertinent contractual clauses in the contract document itself or provide the appropriate statement which identifies the additional Requirements. Provide a copy of the requirements to the CSO. Use Item 13 if additional space is needed.)

SEE CONTINUATION PAGE

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the CSO.

(If Yes, explain and identify specific areas and government activity responsible for inspections. Use Item 13 if additional space is needed.)

☒ No ☐ Yes

SEE CONTINUATION PAGE

16. GOVERNMENT CONTRACTING ACTIVITY (GCA) AND POINT OF CONTACT (POC)

a. GCA NAME USSOCOM/SOF AT&L-SR	b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE (See instructions.) H92222	c. ADDRESS (Include ZIP Code.) HQ USSOCOM/AT&L-SR 7701 Tampa Point Blvd MacDill AFB, FL 33621
d. POC NAME (See instructions.) Eric Carlin	e. POC TELEPHONE (Include Area Code.) 813-826-3124	f. EMAIL ADDRESS (See instructions.) eric.carlin@socom.mil

17. CERTIFICATION AND SIGNATURES. 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)(3) (10 U.S.C. § 130b), (b)(6)	b. TITLE	c. ADDRESS (Include ZIP Code.) HQ USSOCOM/AT&L-SR 7701 Tampa Point Blvd MacDill AFB, FL 33621
d. AAC OF THE CONTRACTING OFFICE (See instructions.) N/A	e. CAGE CODE OF THE PRIME CONTRACTOR (See instructions.) N/A	
f. TELEPHONE (Include Area Code.) (b)(3) (10 U.S.C. § 130b), (b)(6)	g. EMAIL ADDRESS (See instructions.)	h. DATE 20180626
		i. SIGNATURE (b)(3) (10 U.S.C. § 130b), (b)(6)

18. REQUIRED DISTRIBUTION BY THE CERTIFYING OFFICIAL

☒ a. CONTRACTOR ☒ f. OTHERS AS NECESSARY (If more room is needed, continue in Item 13 or on additional page if necessary.)
☐ b. SUBCONTRACTOR
☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
☒ e. ADMINISTRATIVE CONTRACTING OFFICER
 HQ USSOCOM SMO/SSO

CONTINUATION PAGE**13. SECURITY GUIDANCE** *(Continued)*

The Contracting Officer's Representative/Program Manager listed in Item 17 will provide a copy of all applicable security directives for this contract. Appropriate applicable HQ USSOCOM security directives, regulations, and standard operating procedures will be provided by the requiring agency (normally through the Performance Monitor or Component/Theater Special Operations Command COR/PM). Upon completion or termination of the classified contract, or sooner when the purpose of the release has been served, the contractor will return all classified information (furnished or generated) to the source from which received unless retention or other disposition instructions are authorized in writing by the USSOCOM Government Contracting Agency/Activity. Furthermore, the contractor will account for and return all Common Access Cards (CACs) to Contracting Officer's Representative, Program Manager, or Trusted Agent upon completion or termination of the classified contract, termination of employment, or suspension of classified clearance or access of any contractor employee. Security badges, installation entry passes/vehicle decals issued to contractor personnel will be returned to the appropriate issuing office as required.

SEE CONTINUATION PAGE

Additional persons assisting with completion of form *(signatures and titles)*

(b)(3) (10 U.S.C. § 130b), (b)(6)

Reviewed/Approved
HQ USSOCOM Industrial Security
26 June 2018

14. ADDITIONAL SECURITY REQUIREMENTS. *(Continued)*

While performing duties at USSOCOM, Component (JSOC, AFSOC, NSWC, MARSOC, or USASOC), Theater Special Operation Command (SOCNORTH, SOCCENT, SOCEUR, SOCPAC, SOCSOUTH, SOCAFRICA, or SOCKOR) or other U.S. Government owned and operated facilities, the contractor will adhere to the applicable Information Security Program, ADP and DODIIS Programs, Physical Security Program, Industrial Security Program, and SCI/SAP Program (if applicable). Prior approval of the contracting activity is required for subcontracting. Access to intelligence information requires special briefings and a U.S. Government clearance at the appropriate level.

Training Requirement: Contractors performing on this contract at military installations are required to conduct command and unit specific security training (Initial/Refresher INFOSEC, OPSEC, EMSEC, AT/FP, Intelligence Oversight, etc.). This training will be provided by the responsible military organization.

15. INSPECTIONS. *(Continued)*

Defense Security Service is relieved of all inspection responsibility within USSOCOM, Component (JSOC, AFSOC, NSWC, MARSOC, or USASOC), Theater Special Operation Command (SOCNORTH, SOCCENT, SOCEUR, SOCPAC, SOCSOUTH, SOCAFRICA, SOCKOR) and other U.S. Government owned and operated facilities but retains responsibility for all non-SCI classified material released to or developed under the contract and held within the contractor's facility.

CONTINUATION PAGE

Ref 2b: Subcontracting of this effort must be approved by HQ USSOCOM prior to award. Forward requests and draft Subcontract DD FM 254s to the Certifying Official identified in Item 17 and USSOCOM Industrial Security (IndustrialSecurity@socom.mil). *(IAW USSOCOM R 380-9, Industrial Security, please allow 10 duty days for review/approval).*

Ref 7: See guidance in Ref 2b.

Ref 8: Performance Locations (Continued):

<u>Location</u>	<u>CAGE Code</u>	<u>Cognizant Security Office</u>
Mastodon design LLC 176 Anderson Ave (b)(7)(F) Rochester NY 14607	6ZZG2	New York Field Office (IOFNN) 1600 Stewart Avenue (b)(7)(F) Westbury, NY 11590 (b)(6)
HQ USSOCOM/AT&L-SR 7701 Tampa Point Blvd MacDill AFB, FL 33621	N/A	HQ USSOCOM/SOCS-Z-SM 7701 Tampa Point Blvd MacDill AFB, FL 33621 (b)(3) (10 U.S.C. § 130b), (b)(6)

Item 13 Security Guidance. (Continued):

Ref 10e(1): See attached *SCI Addendum*.

Ref 10j: Controlled Unclassified Information (CUI) provided under this contract shall be safeguarded as specified in the *FOUO Addendum* included with this specification.

Ref 11c: The contractor requires access to classified source data up to and including TOP SECRET in government facilities and SECRET in the contractor's facility in support of the work effort. Contractor will reference the appropriate security classification guidance when generating or deriving classified material or hardware. All classified information received or generated will be properly stored and handled according to the markings on the material. All classified information received or generated is the property of the U.S. Government. At the termination or expiration of this contract, the U.S. Government will be contacted for proper disposition instructions.

Ref 11d: Contractor must provide adequate storage at their facility for classified hardware to the level of SECRET.

Ref 11i: Controlled Unclassified Information (CUI) provided under this contract shall be safeguarded as specified in the *FOUO Addendum* included with this specification.

Ref 11m: Access to all USSOCOM facilities requires contractors to possess a minimum of a SECRET clearance.

CONTINUATION PAGESCI ADDENDUM

This supplement applies to:

Prime Contract Number: H92222-14-C-0026 REV 5

Delivery/Task Order Number: N/A

Subcontract Number: N/A

Expiration Date: 22 April 2019

The following controls will apply to Sensitive Compartmented Information (SCI) provided under this contract.

1. **Item 10e (2):** Security clearances for contractors working within SCIF spaces must be adjudicated meeting Intelligence Community Policy Guidance (ICPG) 704.1, 704.2, 704.3, 704.4, 704.5 eligibility requirements. Prior approval of the contracting activity is required for sub-contracting. Access to intelligence information requires special briefings and a final U.S. Government clearance at the appropriate level.
2. **Item 13:** Department of Defense (DOD) Manual 5105.21, Volumes 1-3, Intelligence Community Policy Guidance (ICPG) 704.1, 704.2, 704.3, 704.4, 704.5, Intelligence Community Standard (ICS) 705-1&2 including the Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities (IC Tech Spec-for ICD/ICS 705, and Headquarters, United States Special Operations Command (HQ USSOCOM) 380-6, provide the necessary guidance for physical and information security measures and are part of the SCI security specifications for the contract.
3. **Item 13:** Inquiries pertaining to classification guidance will be directed to the responsible USSOCOM Contracting Officer's (b)(3) (10 U.S.C. § 130b), (b)(6)
4. **Item 13:** All SCI furnished to the contractor in support of this contract / delivery / task order remains the property of the DOD or the agency or command that releases the information. Upon termination of the contract, all furnished SCI will be returned to the HQ USSOCOM Special Security Office (SSO) or the prime contractor.
5. **Item 14:** This contract / delivery / task order requires that TEN (10) contract billets be established in order to fulfill the contractual obligations incurred. Access will be granted by the government agency. Upon completion or cancellation of the contract, the Contractor SSO (CSSO) will debrief or notify the HQ USSOCOM SSO to debrief all personnel not required for contract closeout and those billets will be disestablished.
6. **Item 14:** Names of contractor personnel requiring access to SCI and justification for SCI billets will be submitted to HQ USSOCOM SSO after contract monitor coordination. Billet justifications will include the contract statement of work. If a Single-Scope Background (SSBI) Investigation has not been completed upon approval of billets by the HQ USSOCOM SSO, the CSSO will submit necessary forms to the Personnel Security Management Office for Industry (PSMO-I) for an SSBI. An SSBI and access to SCI will comply with the National Industrial Security Program Manual. Upon completion of the SSBI, a nomination for SCI access will be submitted to HQ USSOCOM SSO.
7. **Item 14:** The CSSO will advise HQ USSOCOM SSO, through the contract monitor, upon reassignment of personnel to other duties not associated with this contract.
8. **Item 14:** The CSSO must coordinate with the SCI contract monitor before subcontracting any portion of SCI efforts involved in the contract. A separate DD Form 254 for the subcontractor will be processed and a copy provided to HQ USSOCOM SSO.
9. **Item 14:** The contractor will not use references to SCI access, even by unclassified acronyms, in advertisements, promotional efforts, or recruitment of employees.
10. **Item 14:** All SCI work will be performed at the locations specified below and in subsequent Task Orders.
 - a. HQ USSOCOM
11. **Item 15:** HQ USSOCOM SSO has exclusive security responsibility for all SCI released to the contractor or developed under this contract. Defense Intelligence Agency and HQ SSO Socom retain authority for all inspections of the contractor to ensure compliance with SCI directives, regulations, and instructions.

CONTINUATION PAGE

12. In accordance with DODM 5105.21 Volume 1-3, the following activity is designated User Agency Special Security Office for SCI requirement:

**HQ USSOCOM
Special Security Office
7701 Tampa Point Boulevard
MacDill AFB, Florida 33621-5323**

**Telephone:
Commercial**

(b)(3) (10 U.S.C. § 130b), (b)(6)

(b)(3) (10 U.S.C. § 130b), (b)(6)

**Reviewed/Approved
HQ USSOCOM SSO Industrial Security
26 JUNE 2018**

CONTINUATION PAGE**PROTECTING "FOR OFFICIAL USE ONLY" (FOUO) INFORMATION**

(Updated June 2014)

1. GENERAL:

- a. The "For Official Use Only" (FOUO) marking is assigned to information at the time of its creation in a DOD User Agency. It is not authorized as a substitute for a security classification marking but is used on official government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (FOIA).
- b. Other non-security markings, such as "Limited Official Use" and "Official Use Only" are used by non-DOD User Agencies for the same type of information and should be safeguarded and handled in accordance with instruction received from such agencies.
- c. Use of the above markings does not mean that the information cannot be released to the public under FOIA, only that it must be reviewed by the Government prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions of it

2. MARKINGS:

- a. Unclassified documents containing FOUO information will be marked "UNCLASSIFIED//For Official Use Only" or "U//FOUO" at the bottom of the front cover (if any), on the first page, on each page containing FOUO information, on the back page, and on the outside of the back cover (if any). Each paragraph containing FOUO information shall be marked as such.
- b. Within a classified document, an individual page that contains both FOUO and classified information will be marked at the top and bottom with the highest security classification of information appearing on the page. Individual paragraphs shall be marked at the appropriate level be it classified, unclassified, or FOUO. An individual page that ONLY contains FOUO and unclassified information shall be marked "FOR OFFICIAL USE ONLY" or the highest classification of the entire document at the top and bottom of the page. If an individual portion contains FOUO information but no classified information, the portion will be marked, "FOUO."
- c. Mark other records, such as computer print outs, photographs, films, tapes, or slides "FOR OFFICIAL USE ONLY" so that the viewer knows the record contains FOUO information.
- d. Removal of the "For Official Use Only" marking can only be accomplished by the originator or other competent authority. When the "For Official Use Only" status is terminated, all known holders will be notified to the extent practical.

3. DISSEMINATION: "For Official Use Only" information may be disseminated between officials of DOD Components, DOD contractors, consultants, and grantees to conduct official business for the DOD. FOUO information may also be passed to officials in other departments and agencies of the executive and judicial branches to fulfill a government function. Recipients shall be made aware of the special handling instructions detailed in this document and that it's exempt from public disclosure under the FOIA utilizing the following statement: "This document contains information EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA".

4. STORAGE: During working hours, "For Official Use Only" information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During nonworking hours, the information shall be stored to preclude unauthorized access. Filing such material with other unclassified records in unlocked files or desks, is adequate when internal building security is provided during nonworking hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after- hours protection or the material can be stored in locked receptacles such as file cabinets, desks, or bookcases.

5. TRANSMISSION: "For Official Use Only" information may be sent in the following ways:

- a. Mail - FOUO may be sent via first-class mail or parcel post. Bulky shipments may be sent by fourth-class mail.
- b. Fax - Normally FOUO may be sent over facsimile equipment. To prevent unauthorized disclosure the following should be considered: Use of special cover sheets, location of fax machines (both ends), and whether authorized personnel are around to receive FOUO information.
- c. E-Mail/Websites E-mail may be used on approved secure communication systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI) or transport layer security (e.g., https).

****Make sure documents/methods that transmit FOUO material call attention to any FOUO attachments. ****

6. DISPOSITION: When no longer needed, FOUO information must be disposed of in a way that will preclude its disclosure to unauthorized individuals.

7. UNAUTHORIZED DISCLOSURE: Unauthorized disclosure of "For Official Use Only" information does not constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions and disciplinary action may be taken against those responsible.