

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>		1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED TOP SECRET b. LEVEL OF SAFEGUARDING REQUIRED NONE	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable) <input checked="" type="checkbox"/> a. PRIME CONTRACT NUMBER H92222-13-D-0005, Task Order 010		3. THIS SPECIFICATION IS: (X and complete as applicable) <input type="checkbox"/> a. ORIGINAL (Complete date in all cases) Date (YYYYMMDD) 20141215 <input checked="" type="checkbox"/> b. REVISED (Supersedes all previous specs) Revision No. 1 Date (YYYYMMDD) 20151229 <input type="checkbox"/> c. FINAL (Complete Item 5 in all cases) Date (YYYYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO If YES, complete the following: Classified material received or generated under H92222-13-D-0005, Task Order 007 (Preceding Contract Number) is transferred to this follow-on contract			
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____			
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code) a. NAME, ADDRESS, AND ZIP CODE Insitu Corporation 118 East Columbia Point Way Bingen, WA 98605			
b. CAGE CODE 02FP7			
c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) Defense Security Service Tacoma Field Office (IOFWW) 1126 Pacific Ave, 4th Floor Tacoma, WA 98402			
7. SUBCONTRACTOR a. NAME, ADDRESS, AND ZIP CODE			
b. CAGE CODE			
c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)			
8. ACTUAL PERFORMANCE a. LOCATION SEE CONTINUATION PAGE			
b. CAGE CODE			
c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)			
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT Provide Mid-Endurance Unmanned Aircraft System ISR Services for world-wide, 24 hours per day, seven days per week intelligence gathering, target surveillance, and reconnaissance (ISR).			
(b)(4)			
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		YES	NO
11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		<input checked="" type="checkbox"/>	<input type="checkbox"/>
b. RESTRICTED DATA		<input type="checkbox"/>	<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>
d. FORMERLY RESTRICTED DATA		<input type="checkbox"/>	<input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION (1) Sensitive Compartmented Information (SCI)		<input checked="" type="checkbox"/>	<input type="checkbox"/>
(2) Non-SCI		<input checked="" type="checkbox"/>	<input type="checkbox"/>
f. SPECIAL ACCESS INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>
g. NATO INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION		<input type="checkbox"/>	<input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION WILL BE HANDLED IAW FOUO Addendum		<input checked="" type="checkbox"/>	<input type="checkbox"/>
k. OTHER (Specify) FP/ACCM NIPRNET/SIPRNET access required at government facilities only.		<input checked="" type="checkbox"/>	<input type="checkbox"/>
l. OTHER (Specify) Access to all USSOCOM facilities requires contractors to possess a minimum of a SECRET clearance.			

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

Requests must be forwarded through the certifying official (block 16), USSOCOM Office of Public Affairs (SOCS-PA), and the Contracting Officer.

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. The contractor may also challenge guidance or the classification assigned to any information or material furnished or generated under this contract; and may submit questions for interpretation of the guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

The Program Manager listed in block 16 will provide a copy of all applicable security directives for this contract. Appropriate applicable command security directives, regulations, and standard operating procedures will be provided by the requiring agency (normally through the Performance Monitor or component command COR). 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 to the appropriate issuing office, all Common Access Cards (CAC), security badges, installation entry passes/vehicle decals issued to contractor personnel upon completion or termination of the classified contract, termination of employment, or suspension of classified clearance or access of any contractor employee.

SEE CONTINUATION PAGE

(b)(3) (10 U.S.C. § 130b), (b)(6)

Reviewed/Approved

(b)(3) (10 U.S.C. § 130b), (b)(6)

USSOCOM Industrial Security

29 December 2015

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. YES NO
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement, which identifies the additional requirements. Provide a copy of the requirements to the Cognizant Security Office. Use Item 13 if additional space is needed.)

SEE CONTINUATION PAGE

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the Cognizant Security Office. YES NO
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

SEE CONTINUATION PAGE

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)(3) (10 U.S.C. § 130b), (b)(6)	b. TITLE MEUAS Program Manager	c. TELEPHONE (Include Area Code) (b)(3) (10 U.S.C. § 130b), (b)(6)
---	-----------------------------------	---

d. ADDRESS (Include Zip Code) HQ USSOCOM SOE AT&L/FW UAS Attn: (b)(3) (10 U.S.C. § 130b), (b)(6) 7701 Tampa Point Blvd MacDill AFB, FL 33621-5323		17. REQUIRED DISTRIBUTION
		<input checked="" type="checkbox"/> a. CONTRACTOR
		<input type="checkbox"/> b. SUBCONTRACTOR
		<input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
		<input type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
		<input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER
		<input checked="" type="checkbox"/> f. OTHERS AS NECESSARY USSOCOM SMO/SSO

DD FORM 254 CONTINUATION PAGE

SECTION 8:

a [REDACTED]
a [REDACTED] (b)(4), (b)(7)(F)

SECTION 13:

Ref 10a: COMSEC security requirements apply. Contractors must forward requests for COMSEC material/information to the appropriate COMSEC officer through the Program Office. The Contractor is governed by DoD 5220.22-NISPM. Access to COMSEC material by personnel is restricted to U.S. citizens holding final U.S. Government clearances. Such information is not releasable to personnel holding only reciprocal clearances. The government Program/Project Manager shall designate the number of personnel requiring cryptographic access. The number will be limited to the minimum necessary and will be on a strict need-to-know basis. Additional COMSEC requirements may be required at non USSOCOM locations/facilities (based on service/command requirements). The Performance Monitor or component command COR at these locations will provide specific information.

- Subcontracting of COMSEC material by a contractor requires prior approval of the contracting activity.
- Access to COMSEC material requires special briefings.
- Access to classified COMSEC material requires a final U.S. Government clearance at the appropriate level.
- Access to COMSEC material may require contractor to complete a counterintelligence (CI) scope polygraph examination.

Ref 10e (1): See SCI Addendum.

Ref 10 j: FOUO information provided under this contract shall be safeguarded as specified in Attachment, Protecting for Official Use Only (FOUO) information.

Ref 10k: ACCM information is governed by DoDM 5200.01 Vol 3, "Information Security Program," Chapter 6, Section 8, "Alternative Compensatory Control Measures (ACCM)," and OSD/C3I Memorandum, 18 April 2003, "Revised Alternative Compensatory Control Measures (ACCM) Guidance"; Focal Point Program information is governed by CJCS Manual 3213.02C, "Focal Point Program Procedures", and supporting documentation for each Focal Point sub-system, including security classification guides, program security plans, and governing directives. Inspections of ACCM information in USSOCOM, Component (JSOC, AFSOC, NSWC, MARSOC, or USASOC), or Theater Special Operation Command (SOCAF, SOCCENT, SOCEUR, SOCPAC, SOCSOUTH, or SOCKOR) owned and operated facilities are under the auspices of the respective Command or Component FPPCO.

Ref 11a: Contractor performance is restricted to government facilities [REDACTED] (b)(7)(F) [REDACTED] Government agency or activity will provide security classification guidance for performance of this contract. Submit visit request to COR and/or Security Management Office for need-to-know verification.

Ref 11f: Contract will be performed at various world-wide locations [REDACTED] (b)(7)(F)

SECTION 14:

While performing duties at USSOCOM, Component (JSOC, AFSOC, NSWC, MARSOC, or USASOC), or Theater Special Operation Command (SOCAF, SOCCENT, SOCEUR, SOCPAC, SOCSOUTH, or SOCKOR) 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 (OPSEC, EMSEC, AT/FP, Etc.). This training will be provided by the responsible military organization.

IA Requirements: Specific Information Assurance requirements may be mandated and are authorized by the responsible command/unit where primary performance location is identified.

SECTION 15:

Defense Security Service is relieved of all inspection responsibility within USSOCOM, Component (JSOC, AFSOC, NSWC, MARSOC, or USASOC), or Theater Special Operation Command (SOCAF, SOCCENT, SOCEUR, SOCPAC, SOCSOUTH, or SOCKOR) 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.

SCI ADDENDUM for MEUAS 1.5 DD Form 254

This supplement applies to:

Prime Contract Number: H92222-13-D-0005

Delivery/Task Order Number: 010 REV 1

Subcontract Number: N/A

Expiration Date: (b)(4)

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 Manual (DoDM) 5105.21 Volumes 1-3, Intelligence Community Policy Guidance (ICPG) 704.1, 704.2, 704.3, 704.4, 7045, 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 contract monitor (b)(3) (10 U.S.C. § 130b), (b)(6) (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 TWELVE (12) 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 Defense Industrial Security Clearance Office (DISCO) 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 in approved SCIFs (b)(7)(F)
11. Item 15: HQ USSOCOM SSO has exclusive security responsibility for all SCI released to the contractor or developed under this contract. DIA and HQ SSO SOCOM retain authority for all inspections of the contractor to ensure compliance with SCI directives, regulations, and instructions.

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

HQ USSOCOM
Special Security Office
7701 Tampa Point Boulevard
MacDill AFB, Florida 33621-5323
Telephone: DSN 299-3631 / Commercial (813) 826-3631

(b)(3) (10 U.S.C. § 130b), (b)(6)

Reviewed/Approved

(b)(3) (10 U.S.C. § 130b), (b)(6)

29 Dec 2015

PROTECTING "FOR OFFICIAL USE ONLY" (FOUO) INFORMATION

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 to the extent that such may be withheld from the public under exemptions 2 through 9 of the FOIA and marked in accordance with 2.c below. As used herein, "FOUO" markings shall only be applied to information described in 5 USC § 552(b), and shall also indicate the applicable FOIA Exemption. Contractor shall apply this Attachment 4A in a manner consistent with its policies implementing Section 15 of the Federal Advisory Committee Act, 5 USC App. § 15 (1997).
- 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. An unclassified document containing FOUO information will be marked "For Official Use Only" 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). No portion markings will be shown.
- 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. If an individual portion contains FOUO information but no classified information, the portion will be marked, "FOUO."
- c. Any "For Official Use Only" information released to a contractor by a DoD User Agency is required to be marked with the following statement prior to transfer.

"This document contains information EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA. Exemptions apply."

- 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: Contractors may disseminate "For Official Use Only" information to their employees and subcontractors who have a need for the information in connection with a classified contract. Contractors must ensure employees and subcontractors are aware of the special handling instructions detailed below.

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 via first-class mail or parcel post. Bulky shipments may be sent by fourth-class mail. DoD components, officials of DoD components, and authorized DoD contractors, consultants, and grantees send FOUO information to each other to conduct official DoD business. Tell recipients the status of such information, and send the material in a way that prevents unauthorized public disclosure. Make sure documents that transmit FOUO material call attention to any FOUO attachments. Normally, you may send FOUO records over facsimile equipment. To prevent unauthorized disclosure, consider attaching special cover sheets, the location of sending and receiving machines, and whether authorized personnel are around to receive FOUO information. FOUO information may be passed to officials in other departments and agencies of the executive and judicial branches to fulfill a government function. Mark the records "For Official Use Only" and tell the recipient the information is exempt from public disclosure under the FOIA and requires special handling. Electronic transmission of FOUO information, e.g., voice, data or facsimile, and e-mail, shall be by approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI), whenever practical.

6. DISPOSITION: When no longer needed, FOUO information must be shredded.

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.