CLASSIFICATION *(When filled in)*: Unclassified

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

RETURN COMPLETED FORM AS DIRECTED IN THE INSTRUCTIONS.

1. CLEARANCE AND SAFEGUARDING

a. LEVEL OF FACILITY SECURITY CLEARANCE (FCL) REQUIRED *(See instructions.)*	b. LEVEL OF SAFEGUARDING FOR CLASSIFIED INFORMATION/MATERIAL REQUIRED AT CONTRACTOR FACILITY
Top Secret	None (See instructions)

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

X	a. PRIME CONTRACT NUMBER *(See instructions.)* H92222-11-D-0017 Task Order 0005	
	b. SUBCONTRACT NUMBER	
	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)* 20120123
X	b. REVISED *(Supersedes all previous specifications.)*	REVISION NO. 003	DATE *(YYYYMMDD)* 20180321
	c. FINAL *(Complete Item 5 in all cases.)*		DATE *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? [X] 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? [X] NO [ ] YES. 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	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (CSO) *(Name, Address, ZIP Code, Telephone)*
Arma Global Corporation 2701 N. Rocky Point Drive (b)(7)(F) Tampa, FL 33607	53N51	Defense Security Services 500 East Zack Street (b)(7)(F) Tampa, FL 33602

7. SUBCONTRACTOR(S) *(Click button to add more subcontractors.)*

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

8. ACTUAL PERFORMANCE *(Click button to add more locations.)*

a. LOCATION(S) *(For actual performance, see instructions.)*	b. CAGE CODE *(If applicable, see instructions.)*	c. COGNIZANT SECURITY OFFICE(S) (CSOs) *(Name, Address, ZIP Code, Telephone) (If applicable, see instructions.)*
492 SOACS 115 Simpson Avenue (b)(7)(F) Hurlburt Field, Florida 32544 MULTIPLE LOCATIONS, SEE BLOCK 13	N/A	SEE BLOCK/ITEM 15 OF THIS FORM

9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT *(Click here if more space is needed.)*

The objective of this contract is to support and maintain current and future command, control, and mission systems (C2MS) for AFSOF organizations.

Period of Performance: 01 Apr 18 - 31 Mar 19

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

X	a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X	f. SPECIAL ACCESS PROGRAM (SAP) INFORMATION
	b. RESTRICTED DATA	X	g. NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION
	c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) *(If CNWDI applies, RESTRICTED DATA must also be marked.)*		h. FOREIGN GOVERMENT INFORMATION
	d. FORMERLY RESTRICTED DATA	X	i. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM) INFORMATION
	e. NATIONAL INTELLIGENCE INFORMATION:	X	j. CONTROLLED UNCLASSIFIED INFORMATION (CUI) *(See instructions.)*
	(1) Sensitive Compartmented Information (SCI) X	X	k. OTHER *(Specify) (See instructions.)* Automated Information Systems NIPRNET, SIPRNET, JWICS, SCAMPI, GIANT, SOIS, Centrix, BICES, any other networks as needed.
	(2) Non-SCI X		

DD FORM 254, NOV 2017 PREVIOUS EDITION IS OBSOLETE. Adobe LiveCycle Designer ES4

CLASSIFICATION *(When filled in)*: Unclassified

CLASSIFICATION *(When filled in)*: Unclassified

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

X	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.)*	X	h. REQUIRE A COMSEC ACCOUNT
	b. RECEIVE AND STORE CLASSIFIED DOCUMENTS ONLY		i. HAVE A TEMPEST REQUIREMENT
	c. RECEIVE, STORE, AND GENERATE CLASSIFIED INFORMATION OR MATERIAL	X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS
	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE (DCS)
	e. PERFORM SERVICES ONLY		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.)*
X	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	X	m. OTHER *(Specify) (See instructions)*
	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		FOCAL Point, NIPRNET, SIPRNET, JWICS, SCAMPI, GIANT, SOIS, Centrix, BICES, any other networks as needed.

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 (NISPOM) or unless it has been approved for public release by 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 here with at least office and phone contact information and if available, an e-mail address. *(See instructions)*

[ ] DIRECT [X] THROUGH *(Specify)*

Info requiring AF or DoD-level review will be forwarded by the entry-level public affairs office through the MAJCOM/DRU Public Affairs Office.

PUBLIC RELEASE AUTHORITY:

Secretary of the Air Force, Office of Public Affairs, Security and Review Division (SAF/PAX), 1690 Air Force Pentagon, Washington DC 20330

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. Click button to add additional pages as needed to provide complete guidance.)*

1. Supported USAF organizations will provide security classification guides and other classification guidance to the contractor as required for contract performance. Contractors will comply with all Hurlburt Field, supported unit and special program requirements. Supported units will provide security requirements and instructions, and will include contractors in the unit Information Security program.
2. Classified markings on all working, draft, and final copies of deliverable material shall be in accordance with DODM 5200.01, Vol 2, and applicable instructions contained in the respective security classification guides.
3. For on-base contractors, the NISPOM security standards will be satisfied by incorporating AFI 16-1404, Air Force Information Security Program, and AFI 16-1406, Air Force Industrial Security Program Management, requirements into the Visitor Group Security Agreement (VGSA).

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

[ ] No [X] Yes *(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 CSO. Use Item 13 or click button if additional space is needed.)*

Provide the information requested by the Notification of Government Security Activity clause and Visitor Group Security Agreements Clause, AFFARS 5352.204-9000, to the Servicing Security Activity indicated in Item 13 above. Refer to the contract document for these clauses. The visitor group will operate per DoDM 5200.01, AFI 16-1404, Hurlburt Field supplements and unit security program operating instructions, plans and procedures.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the CSO. [ ] No [X] Yes

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

Long term visitor groups will be inspected as part of the supported organizations annual Information Security Program Review, conducted by the SSA, while operating on an Air Force Installation. The contractor will comply with the visitor group security agreement provided by the USAF Program/Project Manager at the performance location. The above does not apply to intelligence, SCI and SAP. See attached addendum.

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

a. GCA NAME	b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE *(See instructions.)*	c. ADDRESS *(Include ZIP Code.)*
HQ USSOCOM/SOF AT&L-K	H92222	HQ USSOCOM/SOF AT&L-K, 7701 Tampa Point Blvd, MacDill AFB, FL 33621
d. POC NAME *(See instructions.)*	**e. POC TELEPHONE** *(Include Area Code.)*	**f. EMAIL ADDRESS** *(See instructions.)*
Regina Ferrall	(813) 826-7170	regina.farrell@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 *(Last, First, Middle Initial) (See instructions.)*	b. TITLE	c. ADDRESS *(Include ZIP Code.)*
(b)(3) (10 U.S.C. § 130b), (b)(6)	COR	492 SOACS 115 Simpson Avenue, (b)(7)(F) Hurlburt Field, Florida 32544
d. AAC OF THE CONTRACTING OFFICE *(See instructions.)*	**e. CAGE CODE OF THE PRIME CONTRACTOR** *(See instructions.)*	
H92222	53N51	
f. TELEPHONE *(Include Area Code.)* **g. EMAIL ADDRESS** *(See instructions.)*	**h. DATE**	**i. SIGNATURE**
(b)(3) (10 U.S.C. § 130b), (b)(6)	2018-03-21	(b)(3) (10 U.S.C. § 130b), (b)(6)

18. REQUIRED DISTRIBUTION BY THE CERTIFYING OFFICIAL

X	a. CONTRACTOR	X	f. OTHERS AS NECESSARY *(If more room is needed, continue in Item 13 or on additional page if necessary.)*
	b. SUBCONTRACTOR		
X	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR		
X	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION		
X	e. ADMINISTRATIVE CONTRACTING OFFICER		1 SOW/IPC (Industrical Security Office)

13. SECURITY GUIDANCE *(Continued)*

4. All classified material provided will be safeguarded at all times and returned by the contractor at contract completion. Individuals are responsible for safeguarding classified information entrusted to them.
5. Use only AF certified AIS for performance on base and will comply with all AF AIS procedures. Ref Item 8a.

Ref Item 8a. 1st Special Operations Wing, Hurlburt Field, FL; 27th Special Operations Wing, Cannon AFB. NM; 352d Special Operations Group, Mildendhall AB, UK; 353d Special Operations Group, Kadena AB, Japan; and the 720th Special Tactics Group, Hurlburt Field, FL.
Ref item 10f: The OPR for the SAP is not the office shown in item 13 of this form. However, the contractor requires access to SAP material and must adhere to the special access instructions, requirements, procedures developed by the specific SAP program manager.
Ref Item 10g: Access to NATO information requires a final US Government clearance at the appropriate level. The AFSOC NATO Registry can be contacted at 850-884-2368 or 884-2290.
Ref Item 10k: Secret Internet Protocol Network (SIPRNET) access authorization. The contractor shall not access, download, or further disseminate any information or data that falls outside the scope of execution of the defined contract requirements. In the event any additional access is required, the Program Manager, Contracting Officer Representative, or Security Manager must request modification/revision of the DD Form 254 and/or Statement of Work to the issuing Contracting Officer. Contractor shall prepare and submit all required documentation as required by command policy prior to receiving access.
Ref Item 11a. The highest level of security clearance required for contract performance is Top Secret. Using activities will provide security classification guidance for performance of this contract. The government will oversee the handling and storage of classified information in support of this contract. The government will provide storage capability for all classified material required for this contract. All classified information shall be returned to the government upon termination of the contract

**See attached addendums for items 10a, f, g, j, k and 11j. (Corresponds to items marked in blocks 10 and 11 on page 1)

DD FM 254 Reviewed by:
(b)(3) (10 U.S.C. § 130b), (b)(6)

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

(b)(3) (10 U.S.C. § 130b) (b)(6)

14. ADDITIONAL SECURITY REQUIREMENTS *(Continued)*

Requirements, in addition to ISM requirements, are established for this contract.
Provide the information requested by the Notification of Government Security Activity clause and Visitor Group Agreements Clause. AFFARS 5352.204-9000, to the Servicing Security Activity indicated in Item 13 above. Refer to the contract document for these clauses. The visitor group will operate per DoD 5200.01-M. AFI 16-1404. AFI 16-1406, Hurlburt Field supplements and unit security program operating instructions, plans and procedures. See appropriate addendum. If applicable, See attached addendum for SCI.

15. INSPECTIONS *(Continued)*

None

ADDENDUM to DD FORM 254 (BLOCK 10a)

COMSEC

COMSEC material/information may not be released to DoD contractors without Air Force Cryptological Support Center (AFCSC) approval. Contractors will forward requests for COMSEC to the COMSEC officer through the CAASETA program office. The contractor is governed by appropriate Air Force Security Instructions/Manuals (AFSSI/AFSSM) or Air Force Instructions (AFI). Access to COMSEC material or information is restricted to US citizens holding final U.S. Government clearances and is not releasable to personnel holding only a reciprocal clearance. Personnel requiring COMSEC access will be briefed in accordance with AFMAN 33-283, Change 1 (Communication Security Operations). The Air Force program/project manager will designate the number of personnel requiring COMSEC access. The number will be limited to the minimum necessary and will be on a strict need-to-know basis. If contractor is working within a squadron/unit, the contractor will go through the squadron/units' COMSEC Responsible Officer for the use of COMSEC.

IN PERFORMING THIS CONTRACT:

Contractor may be required to provide storage for classified hardware to the level of Top Secret. The contractor will follow all instructions from AF AFIs, AFSSIs, AFSSMs, and AFMANs

A COMSEC account will be established, if necessary, and COMSEC will be protected per DoD 5220.22-S.

See AFSSI 7700, AFSSI 7702, and AFMAN 33-214v1 for additional guidance and requirements.

The contractor is authorized to use the services of DCS if they have acquired an account through AFCSC. The contracting activity must request DCS services from the Commander, Defense Courier Service, ATTN Operations Division, Ft George G. Meade MD 20755. Only certain classified information qualifies for shipment by DCS. It is the responsibility of the contracting activity to comply with DCS policy and procedures.

REQUIREMENTS:

The requirements of DoD 5220.22-M and NSA/CSS Policy Manual 3-16 are applicable to this effort.

All contractor personnel to be granted access to classified COMSEC information must be U.S. citizens granted FINAL clearance by the government prior to being given access. Immigrant aliens, interim cleared personnel, or personnel holding a contractor granted CONFIDENTIAL clearance are not eligible for access to classified COMSEC information released or generated under this contract without the express permission of the Director, NSA.

Contractor employees or cleared commercial carriers shall not carry classified COMSEC material on commercial passenger aircraft anywhere in the world without the approval of the procuring contracting officer.

No contractor generated COMSEC or government furnished material may be provided to the Defense Technical Information Center (DTIC). Contractor generated technical reports will bear the statement "Not Releasable to the Defense Technical Information Center per DoD Directive 5100-38."

Classified paper COMSEC material may be destroyed by burning, disintegration, chopping or high security crosscut shredding. Cryptographic key tapes must be "terminally" destroyed (destroyed to the point where it cannot be reconstructed) utilizing devices listed on the Evaluated Products List (EPL) for Punched Tape Destruction Devices or the EPL for High-Security Disintegrators. Contact the COMSEC office for a list of approved devices. When a method other than burning is used, all residues must be reduced to pieces 5mm or smaller in any dimension. When classified COMSEC material other than paper is to be destroyed, specific guidance must be obtained from the User Agency.

Unclassified COMSEC information released or generated under this contract shall be restricted in its dissemination to personnel involved in the contract. Release in open literature or exhibition of such information without the express written permission of the Director, NSA, is strictly prohibited.

Recipients of COMSEC information under this contract may not release information to subcontractors without permission of the User Agency.

COMSEC systems requirements and assistance can be found at the following:
Email: 1sow.ia@hurlburt.af.mil
Contact: 1 SOCS/SCXS at 884-5666

LAST REVIEWED/UPDATED
June 2016

ADDENDUM TO DD FORM 254 (BLOCK 10f)

SPECIAL ACCESS PROGRAM INFORMATION

A special access program (SAP) is one which is established and approved by the Secretary of the Air Force to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for Top Secret, Secret, Confidential information. A "CARVE-OUT" is a classified contract awarded by the Air Force in connection with a SAP in which the Servicing Security Activity (SSA) has been relieved of security and/or oversight responsibility in whole or in part. Prior approval of the contracting activity is required for subcontracting. Access to SAP information requires a final U.S. Government clearance at the appropriate level.

All SAP work will be conducted within approved government facilities designated by the local SAP Program Security Officer (PSO) or Program Security Manager (PSM).

Billeted programs and any future SAP access will be billeted through the local PSO or PSM.

Continued access by contractor requires accessed employees to attend initial and recurring security training for SAPs. Training will be conducted by the PSO or PSM at the location where the contractor employee's records are retained.

Courier authorization for SAP materials is granted by the PSO or PSM.

All SAP information will be handled in accordance with National industrial Security Operating Manual (NISPOM) Supplement, the DoD SAP Overprint to the NISPOM Supplement, Joint Air Force Navy (JAFAN) 6/0, 6/3, 6/4, 6/9 and the applicable program security directive (PSD) and Security Classification Guides (SCG) for all SAPs accessed. Facility Standard Operating Procedures (SOP) and System Security Plans (SSP) for assigned SAP facility will be adhered to.

SAP information or materials furnished in support of this contract remain the property of the SAP government organization. Upon completion of this contract, all SAP information and materials provided to or generated by the contractor will be returned to the local PSM. If the material has been superseded or no longer applicable, the PSM will provide disposition instructions to the contractor.

Note: Route all DD Form 254's through the appropriate SAP Officer for coordination/review.

Questions/Concerns with Special Access Program Information must be coordinated in advance with the appropriate SAP Officer.

LAST REVIEWED/UPDATED
JUNE 2016

ADDENDUM TO DD FORM 254 (BLOCK 10g)

NATO INFORMATION

WHAT IS NATO?

1. NATO is an acronym for the North Atlantic Treaty Organization. Member nations have signed the North Atlantic Treaty and the NATO Security Agreement, which obligate them to comply with NATO rules.

2. The Secretary of Defense is the United States National Security Authority for NATO. As such, he is responsible for ensuring that NATO security requirements are implemented throughout the Executive Branch of the United States Government.

WHAT IS NATO INFORMATION?

1. NATO information is information that has been generated by or for NATO, or member nation national information that has been released into the NATO security system. The protection of this information is controlled under the NATO security regulations, and access within NATO is determined by the holder, unless restrictions are specified by the originator at the time of release to NATO.

2. Material received by an agency direct from another NATO member nation may contain either NATO information generated by a NATO element or national information generated by a NATO member nation. If it has been marked "NATO" by the originating nation, it must be assumed to contain information released to NATO, and it is controlled under the NATO Security Program. If the material has a national classification marking and is not marked "NATO" by the originator, DO NOT apply a NATO marking unless you are informed in writing by the originator that the material is intended for NATO and is to be protected under the NATO Security Program. Moreover, the material or the information therein shall not be released into the NATO system without the prior written consent of the originator.

CLASSIFICATION MARKINGS AND CATEGORIES OF NATO INFORMATION:

NATO has four levels of classified information: COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL, and NATO RESTRICTED. Certain NATO information is further categorized as ATOMAL information. NATO also distinguishes official, unclassified information.

ACCESS AUTHORIZATION: Access to classified NATO information requires a final U.S. Government clearance at the appropriate level. Special briefings are required for access to NATO IAW AFI 31-406, *Applying NATO Protection Standards*. Prior approval of the contracting activity is required for subcontracting. Your security official will inform you of your level of access to NATO classified material and whether you are authorized access to ATOMAL information.

REFERENCES:

AFI 31-406, *Applying NATO Protection Standards*.
DoD Directive 5100.55, *United States Security Authority for North Atlantic Treaty Organization*
AFPD 31-4, *Information Security* and supplement United States Security Authority for NATO Affairs
USSAN Instruction 1-69, *United States Implementation of NATO Security Procedures*

NATO requirements and assistance can be found by calling the AFSOC NATO Registry (AFSOC/A6) at 850-884-2368 or 850-884-2290.

LAST REVIEWED/UPDATED
June 2016

ADDENDUM TO DD FORM 254 (BLOCK 10j)

FOR OFFICIAL USE ONLY (FOUO)

(*References: DoD Manual 5200.01, Volume 4, February 24, 2012 and DoD Directive 5400.7/Air Force Supplement, 22 July 1999*)

1. **GENERAL**: "For Official Use Only (FOUO)" is a designation that is applied to **unclassified** information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA) (reference (g)). The FOIA specifies nine exemptions that may qualify certain information to be withheld from release to the public if, by its disclosure, a foreseeable harm would occur. FOUO is information that has not been given a security classification pursuant to the criteria of an Executive Order. Additional information on FOUO may be obtained by contacting the User Agency. FOUO is assigned to information at the time it is created in a DoD Agency or derivatively.

2. **MARKING**:

a. FOUO information received **(released by a DoD component)** should contain the following marking, when received: ***THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER FOIA. EXEMPTION(S) ___ APPLIES/APPLY.***

b. Information that has been determined to qualify for FOUO status should be indicated by markings when included in documents and similar material. Markings should be applied at the time documents are drafted, whenever possible, to promote proper protection of the information. Unclassified documents and material containing FOUO information shall be marked as follows:

> "Documents will be marked "FOR OFFICIAL USE ONLY" at the bottom of the front cover (if there is one), the title page (if there is one), the first page, and the outside of the back cover (if there is one). Pages of the document that contain FOUO information shall be marked "FOR OFFICIAL USE ONLY" at the bottom. Each paragraph containing FOUO information shall be marked as such. Material other than paper documents (for example, slides, computer media, films, etc.) shall bear markings that alert the holder or viewer that the material contains FOUO information."

c. Within a classified document, an individual page that contains both FOUO and classified information shall 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 classification level, as well as unclassified or FOUO, as appropriate. An individual page that contains FOUO information but no classified information shall be marked "FOR OFFICIAL USE ONLY" at the top and bottom of the page, as well as each paragraph that contains FOUO information. NOTE: For "production efficiency" the entire document may be marked top and bottom with the highest level of classification contained within it, as long as every paragraph is marked to reflect the specific classification of the information it contains.

LAST REVIEWED/UPDATED
June 2016

ADDENDUM TO DD FORM 254 (BLOCK 10k)

AUTOMATED INFORMATION SYSTEMS

1. This section outlines the requirements, procedures and Air Force publications that must be adhered to by contractors as a condition of use of Hurlburt Field Automated Information Systems (AIS) and Local Area Networks (LAN).

2. Cybersecurity practices are the actions that protect information and information systems by ensuring their continued availability, integrity, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating disaster recovery capabilities to ensure continuity of operations under all conditions.

3. Key publications governing the use and security of AF AIS are listed below. Many include additional publications by reference, which are equally applicable.

- AFSSI 7700, Emission Security
- AFI 33-200, Air Force Cybersecurity Program Management
- AFI 33-210, Air Force Certification and Accreditation (C&A) Program (AFCAP)
- AFMAN 33- 152, User Responsibilities and Guidance for Information Systems
- AFI 10-712, Cyberspace Defense Analysis (CDA) Operations and Notice and Consent Process

4. All personnel are required to safeguard information and information systems against unauthorized access, modification, destruction or disclosure.

5. Per the Hurlburt Field NIPRnet System Security Authorization Agreement (SSAA), contractor owned hardware and software will not be connected to Hurlburt Field unclassified or classified LAN.

6. Non-Air Force wireless network devices are forbidden on Hurlburt Field.

7. All portable electronic devices (PED) are prohibited from use or possession within Hurlburt Field buildings where classified information is processed, stored or discussed.

8. All information systems, software, and/or enclaves operating on Hurlburt Field must be certified and accredited through the DoD Information Assurance Certification and Accreditation Program (DIACAP) prior to being implemented or connected to a network.

9. The 1 SOW Cybersecurity Office is the source for cybersecurity related information.
- Email: 1sow.ia@hurlburt.af.mil
- Contact: 1 SOCS/SCXS at (850) 884-6605

LAST REVIEWED/UPDATED
June 2016

d. Mark other records, such as computer print outs, photographs, films, tapes, or slides 'FOR OFFICIAL USE ONLY" so that the receiver or viewer knows the record contains FOUO information.

e. Mark each part of a message that contains FOUO information. Unclassified messages containing FOUO information must show the abbreviation "FOUO" before the text begins.

3. **ACCESS:** Access to FOUO Information. FOUO information may be disseminated within the DoD Components and between officials of the DoD Components and DoD contractors, consultants, and grantees as necessary in the conduct of official business. FOUO information may also be released to officials in other Departments and Agencies of the Executive and Judicial Branches in performance of a valid Government function. (Special restrictions may apply to information covered by the Privacy Act, reference (h).) Release of FOUO information to Members of Congress is covered by DoD Directive 5400.4 (reference (gg)) and to the General Accounting Office by DoD Directive 7650.1 (reference (ll)).

4. **DISSEMINATION**: FOUO may be disseminated between officials of DoD Components, DoD contractors, consultants and grantees to conduct official business for DoD. Recipients shall be made aware of the status of such information **and transmission shall be by means that preclude unauthorized public disclosure**. FOUO documents and material transmitted outside the Department of Defense must bear an expanded marking on the face of the document so that non-DoD holders understand the status of the information. A statement similar to this one should be used:

"This document contains information exempt from mandatory disclosure under the F0IA. Exemption(s) _____ apply."

5. **TRANSMISSION**: FOUO information shall be transmitted in a manner that prevents disclosure of the contents. When not commingled with classified information, it may be sent via first-class mail or parcel post. Bulky shipments, i.e. testing materials, that otherwise qualify under postal regulations, may be sent by fourth-class mail. FOUO information may also be sent over facsimile equipment; however, when deciding whether to use this means, balance the sensitivity of the records against the risk of disclosure. Consider the location of sending and receiving machines and ensure authorized personnel are available to receive the FOUO information as soon as it is transmitted. Transmittal documents shall call attention to the presence of FOUO attachments. FOUO information may also be sent via e-mail, if it is sent via a system that will prevent unintentional or unauthorized disclosure.

6. **STORAGE**: To safeguard FOR OFFICIAL USE ONLY records during normal duty hours, place them in an out-of-sight location if your work area is accessible to persons who do not have a valid need for the information. After normal duty hours, store FOUO records to prevent unauthorized access. File them with other unclassified records in unlocked files or desks when normal internal building security is provided. When there is no internal building security, locked buildings or rooms normally provide adequate after-hours protection. If such protection is not

considered adequate, FOUO material shall be stored in locked containers such as file cabinets, desks, or bookcases. *Expenditure of funds for security containers or closed areas solely for the protection of FOUO data is prohibited.*

7. **DESTRUCTION**: When no longer needed, FOUO information shall be disposed of by any method that will preclude its disclosure to unauthorized individuals. Destruction of all FOUO, Unclassified, and Official Business related paper products on Hurlburt field is accomplished by shredding.

8. Direct any and all questions concerning FOUO to the 1 SOW/IPI Office at 884-4322.

LAST REVIEWED/UPDATED
June 2016

ADDENDUM TO DD FORM 254 (BLOCK 11j)

OPERATIONS SECURITY

1. This section outlines the requirements and procedures necessary for contractors to provide Operations Security (OPSEC) protection for AFSOC's Critical Information (CI).

2. OPSEC is the process of analyzing friendly actions attendant to military operations and other activities to:

- Identify those actions that can be observed by adversary intelligence systems.
- Determine which of those action are indicators to hostile intelligence systems which they can obtain and interpret or piece together to derive critical information in time to be useful for adversaries planning.
- Develop, select and execute countermeasures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

3. OPSEC principles are used to help assigned personnel:

- Maintain a continuing awareness of adversary interest in SOF actions and adversary intelligence collection capabilities.
- To understand the need to identify and protect unclassified indicators that reveal sensitive information.
- To evaluate the effectiveness of OPSEC measures taken to preclude or reduce adversary acquisition and exploitation of sensitive information.

4. Our objectives are:

- Protect planned operational activities by preventing the inadvertent disclosure of unclassified information relating to or revealing a possible classified operation.
- To preserve secrecy concerning specific scenario events and a USSOCOM or AFSOC response to these events.
- To identify OPSEC vulnerabilities and recommend protective measures which will serve to enhance the security of future operations.

5. AFSOC employed contractors will be OPSEC in-briefed by the assigned unit/directorate's OPSEC program manager/coordinator on the unit/directorate's OPSEC requirements within 30 days of assignment. Individual training will be developed and applied as required by the level of contact with AFSOC critical information.

6. Unit OPSEC requirements, Critical Information Lists (CILs) and assistance can be found by contacting the unit specific OPSEC coordinator.

7. OPSEC requirements and assistance can be found at the following:

- AFI 10-701, *Operations Security (OPSEC)*
- Email: 1sow.io@us.af.mil
- Contact: 1 SOW/IO at 884-4565

LAST REVIEWED/UPDATED
June 2016

ADDENDUM TO DD FORM 254 (BLOCK 11M)

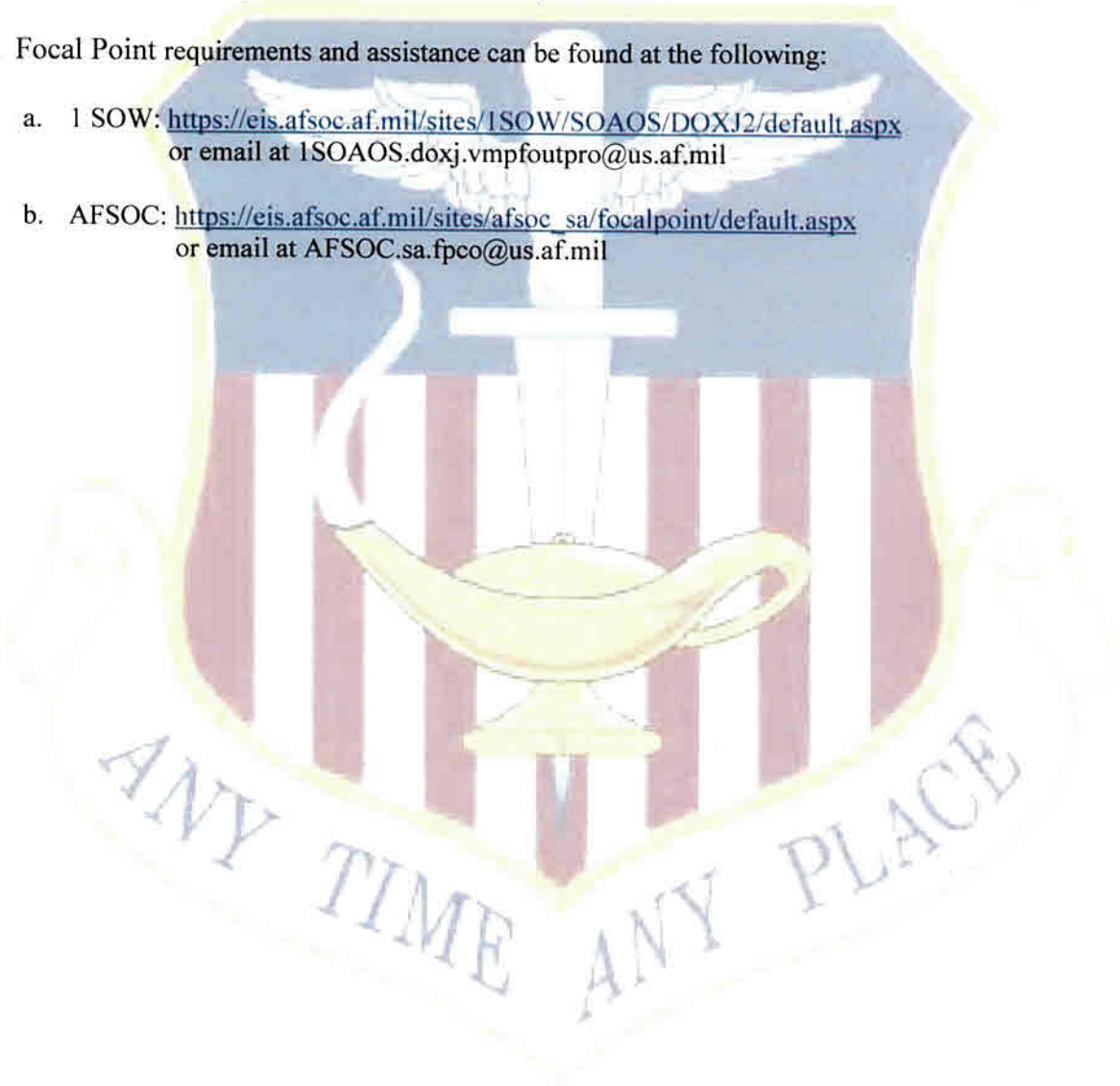
FOCAL POINT

1. For access to Focal Point, contractors must be verified to have a "need to know" and a proper security clearance. After proper vetting, contractors may be briefed into Focal Point and will be entered into USSOCOM's Need-to-Know database (NTKMM). Contractors are permitted access to Focal Point they are cleared to in the performance of their contract. During out processing, the contractor's assigned unit will coordinate with the Focal Point Control Office to schedule debriefing. The FPCO will remove the contractor from the Need-to-Know database (NTKMM). The assigned unit will then notify the COR of read out from Focal Point.

2. Focal Point requirements and assistance can be found at the following:

   a. 1 SOW: https://eis.afsoc.af.mil/sites/1SOW/SOAOS/DOXJ2/default.aspx
   or email at 1SOAOS.doxj.vmpfoutpro@us.af.mil

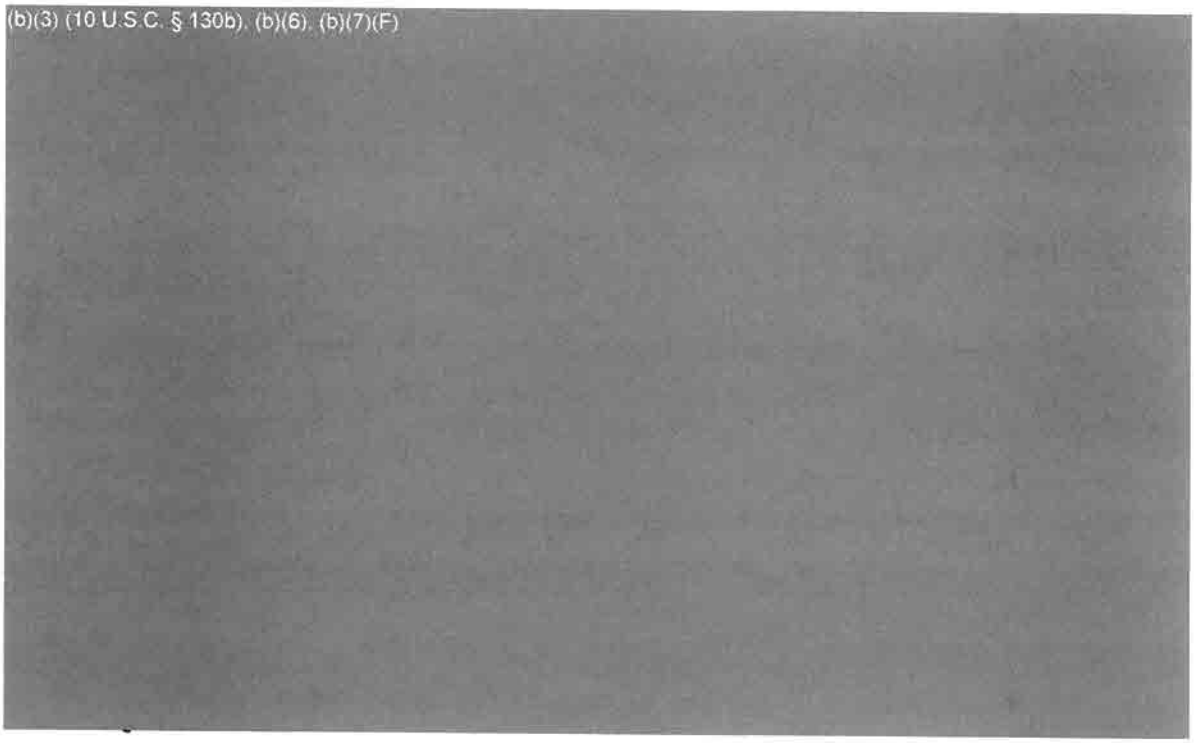
   b. AFSOC: https://eis.afsoc.af.mil/sites/afsoc_sa/focalpoint/default.aspx
   or email at AFSOC.sa.fpco@us.af.mil



LAST REVIEWED/UPDATED
July 2016

SENSITIVE COMPARTMENTED INFORMATION ADDENDUM

AIR FORCE SPECIAL OPERATIONS COMMAND



The responsible office for this information is AFSOC/A2S. The information is current as of 16 January 2014. Earlier versions of this document are obsolete and will not be accepted for new/revised contracts.

1. Reference Block 12: Add the following text: "Public release of SCI and / or non-SCI intelligence information is prohibited."

2. Reference Block 13: Contractor is prohibited from using references to SCI accesses, even by unclassified acronyms, in advertising or recruitment media or on the company website without specific, case-by-case approval by SSO AFSOC. (Refer to DCID 6/1, paragraph 7.1) When required, the contractor will derivatively classify documents created in the course of this contract using the procedures and criteria defined in Executive Order 13526, *Classified National Security Information,* (EO 13526) as amended and Information Security Oversight Office Implementing Directive No. 1. Requests for original classification of intelligence information at any classification level or within any compartment will be referred to the AFSOC Special Security Officer. Requests for classification not involving SCI or intelligence will be referred to the AFSOC Security Forces office via the Contracting Officer's Representative (COR). When the contractor creates a classified document from extant classified documents (e.g., derivatively classifies a document), the contractor will incorporate into the finished product a list of all sources used and will apply required security classification markings and handling / control / dissemination / declassification caveats to all working, draft and final copies of classified documents as required by EO 13526. Contractor will comply with the AFSOC requirement for shredding of all paper documents, both classified and unclassified.

3. Reference Block 14: This contract requires access to Sensitive Compartmented Information (SCI). This addendum provides the necessary guidance (obtained from the following applicable Executive Orders, directives and manuals) for physical, personnel, industrial, information and information systems security measures and is part of the SCI security specifications for the contract:

Air Force Policy Directive 14-3, *Control, Protection, and Dissemination of Intelligence Information,* 1 May 1998; DoD Manual (DoDM) 5105.21, Volumes 1-3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security*, October 19, 2012; DoDM 5105.21, Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security*, October 19, 2012; DoDM 5105.21, Volume 3, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security and Special Activities*, October 19, 2012; DoD 5220.22-M, *National Industrial Security Program Operating Manual*, February 28, 2006; Director Central Intelligence Directive (DCID) 6/1, *Security Policy for Sensitive Compartmented Information and Security Policy Manual*, 1 March 1995; DCID 6/6, *Security Controls on the Dissemination of Intelligence Information (Sections V, VI, X, and Annex B only),* June 11, 2001; Executive Order 13526, *Classified National Security Information,* 29 December 2009; *Intelligence Community Authorized Classification and Control Markings Register and Manual*, Administrative update 30 March 2012; Intelligence Community Directive (ICD) 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to SCI*, 1 October 2008; ICD 705, *Sensitive Compartmented Information Facilities*, 26 May 2010; ICD 710, *Classification and Control Markings System*, 11 September 2009; Intelligence Community Policy Guidance (ICPG) 704.2, *Personnel Adjudicative Guidelines for Determining eligibility for*

Access to Sensitive Compartmented Information and Other Controlled Access Program Information, 2 October 2008; ICPG 710.1, *Application of Dissemination Controls: Originator Control (ORCON)*, 25 July 25; Information Security Oversight Office booklet *Marking Classified National Security Information*, December 2010 with Revision 1, January 2012.

4. The Contracting Officer's Representative (COR) for the SCI portion of this contract is:

(b)(3) (10 U.S.C. § 130b), (b)(6)		
Name	**Office Symbol**	**Phone (DSN & Commercial)**

5. All DD Forms 254 prepared for subcontracts involving access to SCI under this contract must be forwarded to the COR for approval and then to SSO AFSOC (AFSOC/A2S, 100 Bartley Street (b)(7)(F) Hurlburt Field, FL 32544) for review and concurrence prior to award of the contract. Inquiries pertaining to classification guidance on SCI will be directed to the COR listed in paragraph 2 above. SCI security management issues shall be directed to SSO AFSOC (AFSOC/A2S, 100 Bartley Street (b)(7)(F) Hurlburt Field, FL 32544; 850-884-6689 or DSN 579-6689).

6. SCI access is subject to U.S. Government review and approval as outlined in the aforementioned SCI security guidance and ICPG 704.2. Upon completion or cancellation of the contract, the supporting SSO will debrief all personnel not required for contract close out and those positions will be disestablished.

7. Names of contractor personnel requiring access to SCI, and justification for SCI access, will be submitted to coordination and action to SSO AFSOC after the COR's concurrence and approval. Upon receipt of written approval from the COR, the company Facility Security Officer (FSO) and/or Contractor Special Security Officer (CSSO) may submit the necessary forms to the Defense Security Service (DSS) for a Single Scope Background Investigation (SSBI) for those personnel nominated for SCI access in accordance with the National Industrial Security Program Operating Manual (NISPOM).

8. The SSO/CSSO can grant access to only those individuals who possess the necessary security clearance and who are actually providing services under the contract. Further dissemination to other contractors, sub-contractors, other government agencies, private individuals or organizations is prohibited in writing by the releasing agency.

9. SCI furnished in support of the contract remains the property of the DoD department or command that released it. All SCI will he returned to the releasing DoD department or command upon completion or cancellation of the contract.

10. Do not release classified information to foreign nationals or immigrant aliens even if they are consultants, U.S. contractors, or employees of the contractor unless the originator of that information has provided written permission in advance.

11. Contractor personnel are accountable for all intelligence (including foreign intelligence) materials released to their custody.

12. Classified information will not be reproduced without advance approval of the releasing agency. If permission is granted, each copy must be protected in the same manner as the original information. The CSSO will not destroy any classified foreign intelligence without advanced approval of the releasing agency.

13. Contractor employees will wear a SCIF identification badge (issued by SSO AFSOC or other appropriate government authority) at all times while within a SCIF under Government control. The badge must be prominently displayed on top of the outer garment and above the wearer's waist. This requirement is in addition to that mandating wear of the base-issued contractor identification badge.

14. Contractor will comply with HQ AFSOC policies concerning the use and/or possession of Portable Electronic Devices (PED) within any AFSOC facility. AFSOC prohibits all non-government PEDs and limits use of government PEDs within AFSOC buildings. Refer to AFSOC Instruction 33-202 (*Portable Electronic Device (PED) Security*) for definitions of PEDs.

14. If a SCI Facility (SCIF) is required for execution of this contract, it must meet all of the physical and TEMPEST requirements in DCID 6/9 or ICD 705, as applicable. All SCI used for this contract shall be stored, handled, and maintained only in an accredited SCIF. If applicable, the SCIF(s) for this contract are located at (provide a general address such as: 99 Special Operations Squadron, Hurlburt Field, FL; ABC Corporation, West Nowhere, FL. DO NOT enter SCIF ID numbers.)

15. Visits. The COR must approve contractor visits and certify the visit is in keeping with the deliverables in the contract. The certification must arrive at the supporting SSO at least five (5) working days prior to travel. Contractor visit notices will be sent via the Joint Personnel Adjudication System (JPAS).

16. Information assurance and electronic processing systems, information systems (computers) and network connectivity require accreditation of the equipment and the associated connectivity.

17. **Reference Block 15:** This contract requires access to SCI. The Defense Intelligence agency and its designees are responsible for all inspections of the SCIF(s) and the SCI security management program in order to ensure compliance with all SCI security regulations and policies. If the contractor must establish a new SCIF for the purposes of this contract, the contractor must request permission to build/accredit a SCIF through the COR who will forward

the request to the supporting SSO. Special Security Officers may conduct a program review of SCI material and SCI program management to ensure protection of AF equities.

18. This contract expires: (Date)

(NOTE: Section "F" of the contract usually provides the Period of Performance. Option years are NOT to be included because an option is not valid until the Government exercises that option.)