DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

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

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: Top Secret

b. LEVEL OF SAFEGUARDING REQUIRED: Secret

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*			3. THIS SPECIFICATION IS: *(X and complete as applicable)*			
☒	a. PRIME CONTRACT NUMBER H92222-11-D-0037		☒	a. ORIGINAL *(Complete date in all cases)*		Date *(YYYYMMDD)* 20110712
☐	b. SUBCONTRACT NUMBER		☐	b. REVISED *(Supersedes all previous specs)*	Revision No.	Date (YYYYMMDD)
☐	c. SOLICITATION OR OTHER NUMBER	DUE DATE (YYYYMMDD)	☐	c. FINAL *(Complete Item 5 in all cases)*		Date *(YYYYMMDD)*

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

Classified material received or generated under USZA22-02-D-0017 **is transferred to this follow-on contract**

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

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

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

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Booz Allen Hamilton, Inc. 8283 Greensboro Drive McLean, VA 22102-4904	17038	DSS Northern Virginia Field Office IOFCC2 14428 Albemarle Point Office, Suite 140 Chantilly, VA 20151-1678

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	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Same as Item 6		

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Provide Information Technology Enterprise Networks support and services to HQ USSOCOM, JSOC, USASOC, NSWC, AFSOC, MARSOC, SOCCENT, SOCEUR, SOCPAC, SOCAFRICOM, SOCSOUTH, SOCJFCOM, Tidewater VA area, and SOCKOR. Period of Performance: 20 June 2011 through 19 June 2016 **(Annual Review of DD Form 254 Required)**

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	☐	☒	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	☐	☒
b. RESTRICTED DATA	☐	☒	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	☒	☐
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	☐	☒	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	☐	☒
d. FORMERLY RESTRICTED DATA	☐	☒	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	☐	☒
e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY	☐	☒
(1) Sensitive Compartmented Information (SCI)	☐	☒	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	☐	☒
(2) Non-SCI	☐	☒	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	☐	☒
f. SPECIAL ACCESS INFORMATION	☒	☐	h. REQUIRE A COMSEC ACCOUNT	☐	☒
g. NATO INFORMATION	☐	☒	i. HAVE TEMPEST REQUIREMENTS	☐	☒
h. FOREIGN GOVERNMENT INFORMATION	☐	☒	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	☐	☒
i. LIMITED DISSEMINATION INFORMATION			k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	☐	☒
j. FOR OFFICIAL USE ONLY INFORMATION WILL BE HANDLED IAW FOUO Addendum	☒	☐	l. OTHER *(Specify)* Access to all USSOCOM facilities requires contractors to possess a minimum of a secret clearance.	☐	☒
k. OTHER *(Specify)* FP/ACCM NIPRNET/SIPRNET/SAP access required at government facilities and NIPRNET access required contractor facility.	☒	☐			

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 [X] 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 local service/component 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 identification badges and/or 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
14 Jul 2011

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. [X] 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 [X] 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.)

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
(b)(3) (10 U.S.C. § 130b), (b)(6)	SITEC PCOR	(b)(3) (10 U.S.C. § 130b), (b)(6)

d. ADDRESS *(Include Zip Code)*
HQ USSOCOM / J61 ITMO
7701 Tampa Point BLVD
MacDill AFB FL 33621-5323

e. SIGNATURE
(b)(3) (10 U.S.C. § 130b), (b)(6)

17. REQUIRED DISTRIBUTION

[X]	a. CONTRACTOR
[ ]	b. SUBCONTRACTOR
[X]	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
[ ]	D. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
[X]	E. ADMINISTRATIVE CONTRACTING OFFICER
[X]	F. OTHERS AS NECESSARY

DD FORM 254 CONTINUATION PAGE

SECTION 13:
Actual performance under this contract will be based on issued Task Orders. Task Order specific security requirements will be provided through a separate DD Form 254.

Ref 10f: All SAP access, if required, will be at government facilities. The following regulations, guides, manuals, instructions and standard operating procedures may apply to work performed under this contract and will be delineated at the task order level: Joint Air Force-Army-Navy (JAFAN) Manual 6/0, Special Access Program Security Manual, Revision 1; JAFAN Manual 6/3, Protecting Special Access Program Information Within Information Systems; JAFAN 6/4, Special Access Program Tier Review Process, Revision 1; JAFAN 6/9 Physical Security Standards for Special Access Program Facilities, with SAPCO Issues Change 2; USSOCOM Manual 380-2, Special Access Program Security Guide; Chairman, Joint Chiefs of Staff Manual 3213.02A, Joint Staff Focal Point Communications Procedures Manual; USSOCOM Manual 380-5, Focal Point Communications Systems Procedures; Chairman, Joint Chiefs of Staff Instruction (CJCSI) 5250.01; Program Specific Security Classification and Procedure Guides. SAP operations and processing associated with this effort will be conducted in facilities specifically approved for SAP processing by the USSOCOM SAPCO, PSO or equivalent component-level SAP Coordination Office (SAPCOORD). Contact the appropriate servicing SAPCO or SAP Coordination Office to verify approved SAP facilities locations. USSOCOM and Component-managed SAPFs and SAP Temporary Secure Working Areas (TSWA) are governed by JAFAN 6/9. Access to SAP information requires employees undergo additional personnel security screening IAW JAFAN 6/4, Special Access Program Tier Review Process. SAP security oversight while in USSOCOM or USSOCOM Component-managed facilities is under the cognizance of the USSOCOM or Component SAPCOORD, as appropriate. Additional SAP security requirements may apply at Component Headquarters locations/facilities based on local component requirements. The Performance Monitor or component command COR at these locations/facilities will provide additional guidance. SAP inspections conducted at approved contractor facilities, if applicable, is under the security oversight of the Defense Security Service (DSS) unless officially relieved of their oversight responsibilities.

Ref 10j: FOUO information/provided under this contract shall be safeguard as specified in the attachment, Protecting for Official Use Only (FOUO) Information.

Ref 10k: ACCM information is governed by DoD 5200.1-R, "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 3213.02B, "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 (SOCCENT, SOCEUR, SOCPAC, SOCSOUTH, Tidewater VA or SOCKOR) owned and operated facilities are under the auspices of the respective Command or Component FPPCO.

Ref 11b: Contractor will receive classified documents for reference only; however, if any classified information is generated in performance of this contract, it shall be derivatively classified and marked consistent with the source material.

SECTION 14:
IA requirements: Specific Information Assurance requirements may be mandated and are authorized by the responsible command/unit sponsoring network accreditation if applicable or where primary performance location is identified.

Contractor will be authorized to courier classified information up to Top Secret in performance of official duties upon approval of and designation by the COR, PM, and/or KO.

AFSOC Requirement: 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 DoD 5200.1-R, AFI 31-401, AFI 31-601, Hurlburt Field supplements and unit security program operating instructions, plans and procedures.

All Security Violations/Incidents will be reported to the respective cognizant security office, facility security officer, contracting officer representative, and contracting officer for this contract.

Contract Number: H92222-11-D-0037 Basic Contract
7 July 2011

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 (FOI A).

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.