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: SECRET
b. LEVEL OF SAFEGUARDING REQUIRED: SECRET

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

	a. PRIME CONTRACT NUMBER	
	B. SUBCONTRACT NUMBER	
X	a. SOLICITATION OR OTHER NUMBER: W31P4Q-04-T-0563	DUE DATE *(YYYYMMDD)*

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

	a. ORIGINAL *(Complete date in all cases)*		DATE *(YYYYMMDD)*
	a. REVISED *(Supersedes all previous specs)*	REVISION NO.	DATE *(YYYYMMDD)*
	a. 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 _____ *(Preceding Contract Number)* 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 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)*
TBD		TBD

7. SUBCONTRACTOR

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

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address and Zip Code)*
TBD		TBD

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT
AMCOM Express for Technical, or Programmatic, or Logistics, or Business and Analytical Support Services

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

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)*

REQUIRING ELEMENT TO THE AMCOM PUBLIC AFFAIRS OFFICE (ATTN: AMSAM-PA)
NO PUBLIC RELEASE OF SAP INFORMATION IS AUTHORIZED.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DOD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of 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.)*

a. This basic contract DD Form 254 establishes eligibility for performance at the full scope of contract services. Authorization for classified access for each task order (TO) will be established by separate TO statement of work (SOW). The SOW paragraph 5.0 (Security) for each TO requiring access will define personnel and facility security clearance types and levels of access for that particular TO. Task orders without security requirements will so state.
b. Specific Security Classification Guides for each TO will be specified in TO SOW paragraph 5.0. Block 10(a-K) and Block 11 (a-1) define collateral security requirements.
c. Access to COMSEC equipment (see block 10a) is authorized for STU III secure communications only to meet general contract requirements and contingencies.
d. Contractor will comply with the ITAR, the National Industrial Security Operating Manual (NISPOM, DoD 5220.22-M).
e. All DD Forms 254 for TO involving non-SCI Intelligence will be prepared by the requiring element and msut be forwarded to the AMCOM Senior Intelligence Office for review and concurrence prior to award (See Block 10e2).
f. Each order requiring access to SAP information will have a separate DD Form 254 issued with the order which specifies security requirements for access to SAP for that order. (See block 10f and 10e(1). Specific security guidance (security classification guide/date and security procedures guide/date) for each SAP involved will be specified in DD Form 254 of the Task Order. Access to Special Access Program (SAP) information will be granted at approved Government facilities/other contractor facilities only. Security procedures specified at facilities where SAP information is accessed will be followed. Contractor is not authorized to discuss, store, generate, or process SAP information in his facility. Contactor personnel SSBI accessed to SAP information will require minimum of SECRET personnel security clearance based on a current (within 5 years) investigation. Contractor personnel accessed to SAP information required in the performance of this contract are subject to random selection for counterintelligence - Scope polygraph examinations in accordance with DoD Directive 5210.48. Failure of selected individuals to submit to polygraph examination may result in access to SA information being suspended.

g. All DD Forms 254 prepared for subcontractors involving access to SAP under this contract effort must be forwared to SAP Program Manager for review and concurrence prior to the award of the subcontract.

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.)

Special Access Program Security Guidance

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.)

Compliance with security requirements for support services provided on Redstone Arsenal will be monitored by appropriate Intelligence and Security Directorate Personnel. Compliance with security requirements of support services provided at contractor facilities will be monitored by DSS.

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)*
H. Monty Hill	Acting Chief, Security Division	256-876-8111

d. ADDRESS *(Include Zip Code)*
Intelligence and Security Directorate
US Army Aviation and Missile Command
Redstone Arsenal, AL 35898

e. SIGNATURE
Monty Hill

17. REQUIRED DISTRIBUTION
☒ a. CONTRACTOR
☒ b. SUBCONTRACTOR
☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
☐ e. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
☒ e. ADMINISTRATIVE CONTRACTING OFFICER
☒ f. OTHERS AS NECESSARY

ATTACHMENT 005

Item 13 Security Guidance (Continuation)

h. "For Official Use Only" Information shall not be disclosed by any AMCOM EXPRESS support services contractor without approval of the TO requiring element.

i. The prime contractor and any subcontractors shall adhere to the Operations Security (OPSEC) provisions of AR 530-1, OPSEC. No OPSEC plan is required as a deliverable data item (See Block 11j).

j. The prime contractor and any subcontractors will use existing authorized workspaces (government, contractor, subcontractor) or justify additional approved classified workspace requirements.

k. The NISPOM provides instructions for handling NATO and Foreign Government information. The following instructions also apply:

1. NATO material releases to the contractor does not become the property of the contractor and may be withdrawn at any time.
2. Upon expiration of the contract all NATO material will be returned to the U.S. Army Aviation and Missile Command NATO Control Officer

l. Any weapons system security classification guide (SCG) applicable to a given technical direction order will be provided under separate cover. Information generated under this contract will be marked in accordance with source documentations and will be marked as follows:

DERIVED FROM: (Source document, multiple sources, or security classification guide, date and POC)
DECLASSIFY ON: Date/event from source document or "Source Marked OADR"
DATE OF SOURCE: (Date of source document or SCG)

m. Contractor access to DTIC, RSIC and STINFO information is restricted to contractual subject matter and SOW performance requirements. SAP information will not be released to DTIC or RSIC. The program/project manager will verify need to know by:

-RSIC-signing a Library card for U.S. citizens and non-U.S. citizens or foreign representatives, requiring the contractor to forward a letter through the Contracting Officer to the Foreign Disclosure Officer, requesting the issuance of a library card.

-DTIC-submission of DD Form 1540 and 1541 to DTIC.

n. Classification guidance must be provided in accordance with AR 380-5, and Executive Order 12958.

o. The contractor is not authorized to release any information to any one not associated with this contract without written consent of the Contracting Officer. Additionally, for release of USG information to non-U.S. citizens and/or foreign representatives, the contractor must obtain an export license and the AMCOM Foreign Disclosure must review all data prior to actual release.

p. Concurrence of the Contracting Officer and the requiring elements Security and Foreign Disclosure Office will be obtained prior to issue of a Limited Access Authorization to a non-U.S. citizen in compliance with the NISPOM. Controlled Unclassified Information as defined in DOD 5200.1R, Appendix C, may be disclosed to U.S. persons who are employed by the prime contractor or subcontractors, or to such employees who are foreign persons when requirements of export control and other laws are met. The contractor is responsible for compliance with all applicable laws and regulations governing access to Classified Information or Controlled Unclassified Information.

q. The contractor is not authorized to release any data to foreign nationals or foreign representatives without an approved export license.

r. Prior to sub-contracting with foreign industry the U.S. contractor will consult with the Contracting Officer (CO) and the requiring elements Security and Foreign Disclosure Office. Foreign sub-contractors

must agree that only citizens of their country or the U.S. will be allowed to perform on the contract. The U.S. contractor is responsible for obtaining export licenses and providing the license number to the CO and ISD.

s. Anticipated completion date of this contract is ____TBD_____.

INSTRUCTIONS FOR COMPLETION OF AMSAM-IS-ID FORM 1

1. Fill in all blocks.

2. If contract is a follow-on or extension, place old contract number to the right of the block checked.

3. State the purpose of the contract and how the Intelligence information will be used in the block "Purpose of Contract".

4. In the block "Responsible government office", put in the command contracting organization. For AMCOM, this will be the AMCOM Acquisition Center. For other organizations, it will be their contracting organization. Put in the name, office symbol, and telephone number of the contract administrator from the Acquisition Center responsible for the applicable contract.

5. The contract monitor in the responsible government office must be shown and his signature must appear in the last block. An alternate contract monitor may be designated and signature block provided in "Purpose of Contract" block.

6. This form must be completed and received by the Intelligence Division prior to any release of Intelligence material, written or oral, to the contractor.

7. Eligibility for receipt of Intelligence material must be granted on a contract-by-contract basis.

8. Execution of this form and its filing with the Intelligence Division (ID) certifies the contractor's NEED-TO-KNOW for this contract.

9. The technical monitor must identify the required Intelligence Material to be forwarded to the contractor on the request for release form (usually assisted by ID representative). For documents, this should be by title, if known. If unknown, or for other products/information, a short description will suffice.

10. The ID will forward all Intelligence materials to the contractor.

11. It shall be understood that an automatic suspense date of 90 days from receipt will be imposed unless designated otherwise by the technical monitor.

12. The contract monitor must request any extension of the use of these materials, or transfer to another contract from the ID.

13. If more than one location for work performance the ID will need a listing of all locations where classified work will be performed. Include classified mailing address, cage code, level of clearance and storage capabilities, and name, address and phone number of Facility Security Officer.

14. A Form 1 is required each time the DD Form 254 is modified; this will eliminate any delays in release of intelligence material.

AUTHORITY: AR-181-1

INTELLIGENCE DIVISION

INTELLIGENCE AND
SECURITY DIRECTORATE

CONTRACTOR'S ELIGIBILITY TO RECEIVE INTELLIGENCE MATERIAL

CONTRACT/RFP TITLE NUMBER	☐ NEW ☐ EXTENSION ☐ FOLLOW -ON
CONTRACTOR NAME	EFFECTIVE DATES OF CONTRACT FROM / TO
SECURITY OFFICER	FACILITY CLEARANCE
MAILING ADDRESS TELEPHONE NUMBER	DATE GRANTED AND BY WHOM
	STORAGE CAPABILITY
PURPOSE OF CONTRACT AND INTELLIGENCE UTILIZATION	
RESPONSIBLE GOVERNMENT OFFICE	TECHNICAL /CONTRACT MONITOR
CONTRACT ADMINISTRATOR	OFFICE SYMBOL PHONE
OFFICE SYMBOL PHONE	SIGNATURE DATE

AMSAM-IS-ID Form 1 – 15 May 2001

AMSAM-IS-ID 25 Sep 2001

Intelligence Addendum to Department of Defense Contract Security Classification Specification (DD Form 254)

1. Reference:

Director of Central Intelligence Directive (DCID) 6/6, Security Controls on the Dissemination of Intelligence Information, 11 July 2001. (S//NF//X1) (See Note)

DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), January 1995.

2. Purpose. In accordance with DCID 6/6 (Reference 1a), this addendum specifies contractor responsibilities for the security of intelligence information released by the Senior Intelligence Officer (SIO), U.S. Army Aviation and Missile Command (AMCOM) under this contract.

3. Security Requirements for Intelligence Information.

Contractors performing duties outside of Government owned or controlled facilities will establish procedures to control all intelligence received, produced, and held by it in accordance with the provisions of the NISPOM (Reference 1b) and this addendum.

a. Contractors performing duties inside a Government owned or controlled facility will follow procedures and policies of the NISPOM and the host organization in accordance with DCID 6/6.

b. Intelligence released to the contractor, all reproductions thereof, and all other material generated based on, or incorporating data therefrom (including authorized reproductions), remain the property of the U.S. Government and may be recalled upon notification by the SIO AMCOM. All reproductions and extractions of intelligence shall be classified, marked, and controlled in the same manner as the original (s).

c. Intelligence released in support of this contract may be used only for that purpose. The contractor is not authorized to disclose further or release intelligence to any of its components or employees not directly engaged in providing services under this contract or to another contractor (including subcontractors) without the prior written authorization of the SIO AMCOM.

NOTE: This document contains information EXEMPT FROM MANDATORY DISCLOSURE under FOIA. Exemption 3 applies.

d. The contractor will not release intelligence to foreign nationals or immigrant aliens (including those employed by the contractor), foreign contractors or subcontractors (including a U.S. subsidiary of a foreign-owned company), foreign governments, of international organizations, unless prior approval is obtained from the SIO AMCOM.

e. Upon contract termination, for all intelligence information released by the SIO AMCOM under this contract, the contractor will:

(1) Return any classified intelligence received or generated in performance of the contract unless the material has been declassified, or

(2) Destroy the intelligence in accordance with the NISPOM and provide AMCOM a copy of the final disposition, or

(3) Request in writing, through the Government contracting activity, SIO approval to retain specified intelligence for use on another contract.

4. Address inquiries/correspondence concerning this addendum to:

COMMANDER
U.S. Army Aviation and Missile Command
ATTN: AMSAM-IS-ID, Bldg 5302
Redstone Arsenal, AL 35898-5000

Or email: Douglas.lee@redstone.army.mil
Telephone: Commercial 256-313-5783
DSN 897-5783

REQUEST FOR RELEASE OF INTELLIGENCE MATERIAL TO CONTRACTORS

TO: AMSAM-IS-ID
ATTN: Sandra Woodard
or May Beasley

FROM: (Name/Phone/Office Symbol)

_____
DATE

CONTRACTOR	INDIVIDUAL	CONTRACT NO.

The undersigned, named as a Contract Monitor in the above reference, requests that the Intelligence Material listed below be forwarded to the contractor specified. The contractor will be allowed to retain this material until _____. The undersigned certifies the contractor's need-to-know for this material.

Signature: _____
Contract Monitor

Document Identification Number	Title or Description of Requested Material

Special Access Program Security Guidance

1. SAP security requirements are contained DOD 5220.22-M, National Industrial Security Program Operating Manual Supplement (NISPOMSUP), the DOD Overprint to the NISPOMSUP, and specific SAP Program Security Procedures Guides and Security Classification Guides. Specific guidance/requirements will be issued with each Task Order requiring access to SAP information.

2. Individual Task Orders requiring SAP access may require the contractor to establish a Special Access Program Facility (SAPF) in order to generate and store SAP information/material at their facility. At a minimum, SAPF must meet the requirements of para 5-802b, Overprint to NISPOM Supplement, to include sound attenuation and intrusion detection system. Specific facility security requirements will be included with each Task Order requiring access to SAP information.

3. Contractor personnel granted access to SAP information must have a security clearance based on a personnel security investigation completed within 5 years of the date of access. For continued SAP access, the investigation must remain current within 5 years.

4. Contractor personnel accessed to SAP information required in the performance of this contract are subject to random selection for Counterintelligence-Scope Polygraph Examinations in accordance with DOD Directive 5210-48. Failure of selected individuals to submit to polygraph examination may result in suspension of access to SAP information.

5. DTIC/NTIC will be used only as a source of information. SAP material will NOT be furnished DTIC/NTIC.

GUIDANCE FOR THE PROTECTION OF
"FOR OFFICIAL USE ONLY" (FOUO) INFORMATION

1. **General.** The **"FOR OFFICIAL USE ONLY" (FOUO)** marking is assigned to information at the time of its creation. It is used to designate official government information that may be withheld from the public under exemption 2 through 9 of the Freedom of Information Act. Use of the marking does not mean that the information cannot be released to the public, 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. **Identification 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 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 is required to be marked with the following statement prior to transfer:

This document contains information EXEMPT FROM MANDATORY DISCLOSURE under 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 know holders will be notified to the extent possible.

3. **Dissemination.** **"FOR OFFICIAL USE ONLY"** information may be disseminated by contractors to their employees and subcontractors who have a need for the information in connection with a classified contract.

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 record 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.

6. **Disposition.** When no longer needed, **FOUO** information may be disposed of by tearing each copy into pieces to preclude reconstructing and placing it in a regular trash container.

7. Unauthorized disclosure of **"FOR OFFICIAL USE ONLY"** does not constitute a security violation but the contracting officer should be informed of any unauthorized disclosure. The unauthorized disclosure of **FOUO** information protected by the Privacy Act may result in criminal sanctions.