DD 254 CONTRACT SECURITY ADDENDUM
DMEA PWS 18-8B7

Reference DD 254 Block 13:

A. General:

1. The contractor is required to abide by several security directives. The following references in paragraph B are guidelines for these directives.
2. Strict adherence to the need-to-know principle for intelligence information applies. Access to intelligence information requires a final US Government clearance at the appropriate level.
3. Violations of the foregoing restrictions that result in unauthorized disclosure of intelligence information shall be immediately reported to the supervising security office.
4. Contractor generated or Government furnished material may not be provided to the Defense Technical Information Center. Contract generated technical reports and briefings will bear the statement "Not Releasable to the Defense Technical Information Center per DoD Instruction S230.24."
5. Classified material received or generated under this contract is not releasable to foreign nationals.
6. Inquiries pertaining to this contract related to the generation and release of material shall be forwarded to the POC specified in the DD254 Block 12.
7. The contractor will ensure any investigation submittal to any investigating agency, has the following address in the "Coordination Copy Address" area: Deputy Director DMEA, 4234 54th Street Bldg 620, McClellan CA, 95652-2100.

B. Specific References:

Reference item 10a: Communications Security (COMSEC) and/or cryptographic requirements apply. A COMSEC account is required to store cryptographic material, as required.

Reference item 10 e(2): Intelligence Information, non-SCI, includes intelligence information and related material, whether written or in any other medium, that has been classified under E.O. 12958, or any predecessor or successor E.O. Intelligence information includes:
a. Foreign intelligence and counter intelligence defined in the National Security Act of 1947, as amended, and in E.O. 12333.
b. Information describing US foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodology used for the acquisition, processing or exploitation of such intelligence; foreign military hardware obtained through intelligence activities for exploitation and the results of the exploitation; and any other data resulting from US intelligence collection efforts.
c. Information on intelligence community protective security programs, for example, personnel, physical, technical, and information security.

Reference item 10 h: Sensitive Foreign government information may be obtained and included during the performance of this contract. The contractor shall determine its nature and relevance; and handle it considering the Foreign government's relationship with the US Government and the sensitivity of the material, or classify it to meet US Government requirements.

Reference item 10 j: The contractor is authorized and may have access to Unclassified information/material identified as "For Official Use Only Information" (FOUO). The contractor is prohibited from further disclosure/dissemination, including posting information to a web site, of this information without the expressed written permission of the POC identified in the DD254 Block 12. Material identified as FOUO shall be safeguarded IAW the guidance contained in DoD 5400.7-R, DoD Freedom of Information Act, Chapter 4, and not the National Industry Security Program Operating Manual.

Reference item 10 k: The contractor is authorized access to and may have access to Unclassified information marked as "Limited Distribution" for the purposes of this award. Foreign nationals are prohibited from access to any information identified as Limited Distribution. The contractor shall follow the restrictions placed upon Limited Distribution material, shall not reproduce Limited Distribution material and shall not release Limited Distribution material without the expressed written consent of the POC identified in DD254 Block 12. Unless directed in writing otherwise, or unless a deliverable under the contract, the contractor shall return or destroy all classified information and material received or generated including classified waste material.

Reference item 11 c: The contractor is authorized to receive and generate classified material up to and including the Top Secret SCI level, with caveats SI, TK, G, and HCS. The contractor will adhere to all directives pertaining to marking, using and storing this classified material.

Reference item 11 d: The contractor is authorized to use and store classified hardware in the performance of this contract. The contractor will adhere to all directives pertaining to proper use and storage of this hardware.

Reference item 11 f: The contractor may require access to classified information at one or more Foreign Government sites or US Government facilities outside the US.

Reference item 11 j: The contractor will take the necessary precautions to ensure that employees who require access are instructed on OPSEC and the protection of sensitive, unclassified information as well as "Critical Unclassified Information" (CUI). The contractor will be familiar with OPSEC and be required to take mandatory OPSEC training. The contractor shall ensure that all OPSEC Unclassified, Sensitive and Critical information is returned or destroyed and in a manner prescribed for FOUO material. Note: The Unclassified directives can be downloaded via the www.dtic.mil/whs/directives web site.

Reference item 11 k: In performance of this contract, the contractor may be required, and is authorized to hand carry or courier classified information up to and including TOP SECRET. The contractor will comply with the appropriate DoD/DIA guidance for hand carry/courier of classified information.

Reference Block 12: Public release of classified information is not authorized. Any unclassified information received or generated under this contract intended for release must be submitted to the POC identified in Block 12 for expressed written release authorization.

C. SCI References:

Reference item 10 e(1): This contract requires access to Sensitive Compartmented Information (SCI); the SCI work under this contract will be conducted at the contractor's SCIF once the SCIF has been accredited. DIA has security inspection responsibility for all SCI and the Defense Security Service (DSS) retains responsibility for all collateral information released or developed under this contract and held within the DoD contract's SCIF. The manuals, regulations and directives listed below provide the necessary guidance for physical, personal, and information security for safeguarding SCI, and are part of the security classification specification for this contract.

1. DOD 5105.21-M-1: SCI Security Manual, Administrative Security
2. DCID 6/1: Security Policy for Sensitive Compartmented Information
    a. ICPM 2006-700-8: Office of the Director of National Intelligence Intelligence Community Policy Memorandum – Intelligence Community Modifications to DCID 6/1 Supplement, "Security Policy Manual for SCI Control Systems"
3. **Reference item 11l**: DCID 6/3: Protecting Sensitive Compartmented Information within Information Systems
4. DCID 6/4: Personnel Security Standards and Procedures Governing Eligibility for Access to SCI
    a. ICPM 2006-700-3: Office of the Director of National Intelligence Intelligence Community Policy Memorandum – Intelligence Community Modifications to ANNEX C, "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information", to DCID 6/4, "Personnel Security Standards & Procedures Governing Eligibility for Access to Sensitive Compartmented Information"
    b. ICPM 2006-700-4: Office of the Director of National Intelligence Intelligence Community Policy Memorandum – Intelligence Community Modifications to DCID 6/4, "Personnel Security Standards & Procedures for Governing Eligiblity for Access to Sensitive Compartmented Information (SCI), Annex A, Standard C – Single-Scope background Investigation-Periodic Reinvestigation (SSBI-PR)"
    c. ICPM 2006-700-5: Office of the Director of National Intelligence Intelligence Community Policy Memorandum – Intelligence Community Modifications to DCID 6/4, "Personnel Security Standards & Procedures for Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," ANNEX F, "Reciprocity of SCI Eligibility Determinations"
    d. ICPM 2006-700-6: Office of the Director of National Intelligence Intelligence Community Policy Memorandum – Intelligence Community Modifications to DCID 6/4, "Personnel Security Standards & Procedures for Governing Eligibility for Access to Sensitive Compartmented Information (SCI)," Pertaining to Expeditious Handling of Issue-Free Personnel Security Cases & Out-of-Date Single-Scope Background Investigations for Continued & Renewed SCI Access
5. DCID 6/9: Physical Security Standards for SCI Facilities
    a. ICPM 2005-700-1: Office of the Director of National Intelligence Intelligence Community Policy Memorandum – Intelligence Community Update to Director of Central Intelligence (DCID) 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)
    b. ICPM 2006-700-7: Office of the Director of National Intelligence Intelligence Community Policy Memorandum – Intelligence Community Modifications to DCID 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)"
    c. ICPM 2007-700-2: Office of the Director of National Intelligence Intelligence Community Policy Memorandum – Intelligence Community Modifications to ANNEX C of Director of Central Intelligence Directive 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)
6. ICD 501: Intelligence Community Directive – Discovery & Dissemination or Retrieval of Information within the Intelligence Community
    a. ICPG 501.1: Intelligence Community Directive – Exemption of Information From Discovery
    b. ICPG 501.2: Intelligence Community Directive – Sensitive Review Board & Information Sharing Dispute Resolution Process
    c. ICPG 501.3: Intelligence Community Directive – Subsequent Use of Information
7. **Reference item 11l**: ICD 503: Intelligence Community Directive – Intelligence Community Information Technology Systems Security Risk Management, Certification & Accreditation
8. ICD 700: Intelligence Community Directive – Protection of National Intelligence
9. ICD 701: Intelligence Community Directive – Security Policy Directive for Unauthorized Disclosures of Classified Information
10. ICD 704: Intelligence Community Directive - Personnel Security Standards & Procedures Governing Eligibility for Access to Sensitive Compartmented Information & other Controlled Access Program Information
    a. ICPG 704.1: Intelligence Community Policy Guidance - Personnel Security Standards & Procedures Governing Eligibility for Access to Sensitive Compartmented Information & other Controlled Access Program Information
    b. ICPG 704.2: Intelligence Community Policy Guidance - Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information & other Controlled Access Program Information

c. ICPG 704.3: Intelligence Community Policy Guidance – Denial or Revocation of Access to Sensitive Compartmented Information, other Controlled Access Program Information, & Appeals Processes
d. ICPG 704.4: Intelligence Community Policy Guidance – Reciprocity of Personnel Security Clearance & Access Determinations
e. ICPG 704.5: Intelligence Community Policy Guidance – Intelligence Community Personnel Security Database Scattered Castles

11. ICD 705: Intelligence Community Directive – Sensitive Compartmented Information Facilities
    a. ICPG 705.2: Intelligence Community Policy Guidance - Construction of Sensitive Compartmented Information Facilities Inside the United States
    b. ICS 705-1: Intelligence Community Standard – Physical & Technical Security Standards for Sensitive Compartmented Information Facilities
    c. **Reference item 11l**: ICS 705-2: Intelligence Community Standard – Standards for the Accreditation & Reciprocal Use of Sensitive Compartmented Information Facilities
    d. IC Tech Spec 705: Technical Specifications for Construction & Management of Sensitive Compartmented Information Facilities
12. ICD 710, Intelligence Community Directive - Classification and Control Markings System