JOINT STAFF INDUSTRIAL SECURITY BLOCK 13 ADDENDUM
JS Contract Number:
Awarded to:
As of: 24 Nov 25

Period of Performance:
Base Year (BY): 25Sep26-24Sep27
Option Year 1 (OY1): 25Sep27-24Sep28
Option Year 2 (OY2): 25Sep28-24Sep29

Contracting Officer Representative (COR):
COR: Dan Evans
Office Code: Joint Staff J7, JDTC
Address: 849 Levy St, Fort Eustis, VA 23604
Telephone Number: (757) 878-6361

	ONLY THE CHECKED PROVISIONS ARE APPLICABLE TO THIS CONTRACT.
	If applicable, each Task Order for this contract will identify the security requirements within the Performance Work Statement. This DD254 indicates the minimum standard for all work and highest standard for some work on the multiple award contract
	Reference Item 1a. Specified positions designated by the Contracting Officer's Representative (COR) or Contract Monitor (CM) will require one of the following background investigations depending on the positions:
	(Check below as applicable)
N/A	**Tier 1**. (Formerly National Agency Check with Inquiries, NACI) Required for positions designated as low risk, non-sensitive and for physical and/or logical access.
N/A	**Tier 2**. Required for moderate-risk positions, non-critical sensitive positions, and positions requiring access Confidential, Secret, and Department of Energy (DOE) "L" level information.
☒	**Tier 3.** Formerly National Agency Check with Inquiries (NACI) and National Agency Check Law and Credit, NACLC) Required for positions designated as non-critical sensitive and/or requiring eligibility to Confidential or Secret Information. Minimum requirement for all Contractor Personnel who occupy a non-critical sensitive position.
	SECRET: All on-site contractor personnel MUST possess a minimum of an Interim Secret or a final SECRET (S) Clearance, as applicable, based on a Tier 3 investigation completed within the last 10 years (in-scope). The clearance must be fully adjudicated at the Secret level and will have an indication of "determined eligibility of "Secret" in DISS. Personnel security clearances (PCLs) must be verifiable in the Defense Information Security System (DISS).
	Controlled by: Joint Staff Controlled by: J7, JDTC CUI Categories: CONTRACT, PROCURE Limited Dissemination Control: FEDCON POC:Daniel Evans

N/A	**Tier 4**. Non-Sensitive High Risk (Public Trust) positions.
☒	**Tier 5.** (Formerly Single Scope Background Investigation, SSBI) Required for special sensitive and critical sensitive and/or positions requiring access to Top Secret, DOE "Q," and Sensitive Compartmented Information (SCI). **TOP SECRET**: Depending on the position a contractor may be required to possess an interim TOP SECRET or a final TOP SECRET clearance with SCI access based on a Tier 5 investigation prior to reporting to any assignment within Joint Staff in order to meet contractual security requirements. The clearance must be fully adjudicated at the Top Secret level and will have an indication of "determined eligibility of Top Secret in DISS. Personnel security clearances (PCLs) must be verifiable in the Defense Information Security System (DISS). **ONSITE:** Percentage of required TOP SECRET positions: 100 Percentage of required TOP SECRET SCI positions: 100 **OFFSITE:** N/A All contractors working at an on-site or off-site location or contractor's facility in support of the **classified** portions of this is contract must currently hold at minimum an Interim **SECRET** clearance. IF SELF-EMPLOYED CONSULTANT: In accordance with DSS Industrial Security Letter ISL 2006-02, 22 Aug 2006, Section 12: personal security clearance (PCL)/ facility security clearance (FCL) requirements for Self-Employed Consultants: "Cleared contractors may process self-incorporated consultants for a PCL in accordance with NISPOM paragraph 2-213 provided the consultant and members of his/her immediate family are the sole owners of the consultant's company, and only the consultant requires access to classified information. In such cases, a FCL is not required. Should other employees of the consultant's company require access to classified information, it would constitute a classified subcontract, and as such, a DD Form 254 must be issued by the prime contractor and the consultant's firm will require an FCL. Self-Employed Consultants with a current in scope PCL do not require a FCL."
☒	**Reference Item 7 (Subcontractor).** Before a Prime Contractor can use a subcontractor or a consultant that requires access to classified information on this contract, approval must be obtained from the JS Contracting Officer (CO) and Contracting Officer Representative (COR), or Contracting Officer Technical Representative (COTR), here after identified as "JS CO/COR/COTR". **A DD 254 can be modified by COR for INDUSEC certification upon notification that the Contracting Officer has approved and assurance that the sub contractor has been properly vetted.** After selection of a subcontractor or a consultant requiring access to classified information in performance of this contract, the Prime Contractor will prepare and submit a DD Form 254 through the JS CO/COR/COTR for "Reviewer Approval" for sub contractor issuance. The INDUSEC Branch Chief will be provided a copy of the sub issued DD 254 signed by the Prime Contractor.
☒	**Reference Item 8 (Actual Performance).** Performance of this contract will be at the contractor's facility and one or more of the following U.S. Government (JS) sites/spaces: **Joint Targeting School** Damneck Annex NAS Oceana Virginia Beach, VA 23460 **Joint Staff Suffolk Complex** 116 Lave View Parkway Suffolk, VA 23435
☐	**Reference Item 10a, 11h (COMSEC).** a. The contractor may require and is authorized to have/receive accountable Government furnished COMSEC information and equipment.

b. **Access to COMSEC information requires special briefings at the contractor's facility. Access to COMSEC material/information is restricted to U.S. citizens holding a final U.S. Government clearance at the appropriate level.** Such information is not releasable to personnel holding only reciprocal clearances. Further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior approval of the JS COR/COR/COTR. If the contractor does not have access to COMSEC information and/or equipment and it is required, contact the DSS/OL CSO for that area; and they will brief the contractor in COMSEC safeguarding requirements.

c. The NSA Central Office or Record has primary responsibility for the auditing of all COMSEC material governed by NSA policy. Refer to National Security Agency/Central Security Service (NSA/CSS) Policy Manual 3-16, Control of Communications Security Material, (Aug 2005) page E-4 for guidance in control and protection of COMSEC material/information. The cognizant DSS/OL security office is responsible for inspecting for compliance with the NISPOM. COMSEC material/information may not be released to DoD contractors without NSA approval.

Only if support is provided by government agency:

Contractor must forward request for COMSEC material/information to the COMSEC custodian **[through the Joint Staff Security Office]**. Non-accountable COMSEC information, though not tracked in the COMSEC material control system, may still require a level or control within a document control system. Work with COMSEC equipment and material will be by direction of the government agent.

☐ **Reference Item 10b and 10d (Restricted Data and Formerly Restricted Data).**

a. Access

(1) Contractor will require access to Restricted Data (RD) and Formerly Restricted Data (FRD). The minimal investigation requirements for access to RD and FRD requires a final Favorable Single Scope Background Investigation (SSBI) for Top Secret/RD, Top Secret/Secret/FRD, Secret/RD and a Favorable National Agency Check with Local Agency Checks and Credit Check (NACLC) for access to Secret/FRD, Confidential/RD, or Confidential/FRD. Contractor personnel must be briefed for CNWDI prior to access.

(2) Requests for access to RD and FRD will be submitted by the contractor to the servicing security office, through the Contracting Officer's Representative (COR), for approval. Contractor will be briefed and have the Department of Energy Form 5631.20, *U.S. Department of Energy Request for Visit or Access Approval*, performed at JS spaces or off-site JS sites approved for briefing RD Programs.

b. Implementation Guidance. Implementing procedures for the RD and FRD programs are contained in DoD Directive 5210.2, *Access to Dissemination of Restricted Data, DoD 5200.1-R, Information Security Regulation*, and *applicable NISP Instructions and manuals*. These publications will be used for dissemination, access, marking, management of information, and briefings.

c. Waivers. Requests for waivers to any requirements in the above publications or other requirements involving Restricted Data will be address through the Joint Staff Security Office, ATTN: Restricted Data Program, 9300 JS Pentagon, Washington, DC 20318-9300 for coordination and approval. Requests shall contain sufficient information to permit a complete and thorough analysis of the impact on the RD and FRD programs.

☐ **Reference Item 10c (Critical Nuclear Weapons Design Information).**

a. Access. Due to the sensitivity of Critical Nuclear Weapons Design Information (CNWDI), access shall be granted to the absolute minimum number of personnel who required access for the accomplishment of assigned responsibilities on a contract (classified or unclassified). The Contracting Officer's Representative will ensure access is granted to the minimum number of employees required

on the strictest need-to-know basis. Due to the importance of such information, special requirements have been established for the control and access.

(1) Contractor will require access to Critical Nuclear Weapons Design Information (CNWDI). The minimal investigation requirements for access to CNWDI requires a final Favorable Single Scope Background Investigation (SSBI) for Top Secret/Restricted Data (CNWDI), Secret/ Restricted Data (CNWDI) and a Favorable National Agency Check with Local Agency Checks and Credit Check (NACLC) for access to Confidential/Restricted Data (CNWDI). Contractor personnel must be briefed for CNWDI prior to access.

(2) Requests for access to CNWDI will be submitted by the contractor to the servicing security office, through the Contracting Officer's Representative (COR), for approval. Contractor will be briefed and have the Department of Energy Form 5631.20, *U.S. Department of Energy Request for Visit or Access Approval*, performed at JS spaces or off-site JS sites approved for briefing RD Programs. If the subcontractor does not have access to CNWDI, contact the Cognizant Security Agency (CSA). The CSA will brief the subcontractor in safeguarding requirements for CNWDI. User Agency approval is required prior to granting CNWDI access on a subcontract.

b. Implementation Guidance. Implementing procedures for the CNWDI programs are contained in DoD Directive 5210.2, *Access to Dissemination of Restricted Data, DoD 5200.1-R, Information Security Regulation*, *and applicable NISP Instructions and manuals.* These publications will be used for dissemination, access, marking, management of information, and briefings. All CNWDI will be accounted for and disposed of in accordance with the NISPOM. (NISPOM Chapter 9, Section 2, Paragraph 9-20)

c. Waivers. Requests for waivers to any requirements in the above publications or other requirements involving Restricted Data will be address through the Joint Staff Security Office, ATTN: Restricted Data Program, 9300 JS Pentagon, Washington, DC 20318-9300 for coordination and approval. Requests shall contain sufficient information to permit a complete and thorough analysis of the impact on the RD and FRD programs.

☒ **Reference Item 10e(1) SCI & (2) Non-SCI**.

a. The Joint Staff is required to abide by several security directives. The following definitions are from these directives.

1. Intelligence Community: U.S. Government agencies and organizations identified in Section 3 of the National Security Act of 1947, as amended. DIA is a designated member of the intelligence community.

2. Intelligence Information: Intelligence information and related material include the following information, whether written or in any other medium, classified pursuant to E.O. 13526 or any predecessor or successor Executive Order:

(a) Foreign intelligence and counter intelligence defined in the National Security Act of 1947, as amended, and in Executive Order 12333.

(b) Information describing U.S. 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 U.S. intelligence collection efforts; and

(c) Information on intelligence community protective security programs, e.g. personnel, physical, technical, and information security.

b. Strict adherence to the need-to-know principle for intelligence information applies. Access to intelligence information requires a FINAL U.S. Government clearance at the appropriate level. SCI access by contractor personnel must be approved in writing by the CO/COR/COTR via justification letter. The Contracting Officer's Representative will ensure access is granted to the minimum number of employees required on the strictest need-to-know basis.

c. Violations of the foregoing restrictions that result in unauthorized disclosure of intelligence information shall be immediately reported to the Joint Staff Security Office and DIA.

d. DIA has security responsibility for SCI released to the contractor or developed under this contract, with one exception. Public release of SCI information is not authorized.

e. Contractor generated or Government furnished material may not 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 Instruction 5230.24.'**

f. All contract personnel requiring access to SCI information must:

(1) Be U.S. citizen,

(2) Have been granted a final TOP SECRET security clearance by the U.S. Government,

(3) Have been approved as meeting ICD 704 criteria by a Government Cognizant Security Agency, and

(4) And have been indoctrinated for the applicable compartments of SCI access PRIOR to being given an access to such information released or generated under this contract.

(5) Immigrant aliens, foreign nationals, or personnel cleared on an interim basis are not eligible for access to classified information released or generated under this contract.

g. Prior to being granted access to Top Secret (TS), Special Access Program (SAP), or Sensitive Compartmented Information (SCI), all DoD Contractor employees must orally attest that they will conform to the conditions and responsibilities imposed by law or regulation on those granted access. They shall attest to understanding fully their responsibilities to protect national security information and to adhere to the provisions stated on Standard Form 312, "**Classified Information Nondisclosure Agreement**" and/or the "**SCI/SAP Indoctrination Form**", after reading the entire Nondisclosure Agreement.

h. SCI information/material received by the contractor under this contract may not be released to subcontractors without permission of the JS CO/COR/COTR.

i. Upon expiration of this contract, the contractor shall request disposition instructions for all project material, both classified and unclassified. **The contractor may be directed to destroy or return the material.** If project material is to be retained by the contractor, every effort should be taken to transfer it to a follow-on contract or similar effort, if applicable. Unless in receipt of written authorization by the JS CO/COR/COTR to retain specific material for a specific period of time, the material shall be returned **or destroyed** as instructed. Any exception to security policy shall be referred to the CSO for coordination with the appropriate agencies and the contracting officer.

j. All contractor SCI work and access will be at an appropriate Department of Defense (DoD) accredited SCI Facility (SCIF) or a SCIF accredited by another U.S. Government Agency and properly covered by a Co-Utilization Agreement (CUA). Prior to processing (receiving, creating, discussing, or storing) SCI information in a non-DIA accredited SCIF, the contractor will ensure a Co-Utilization Agreement has been established.

k. The JS COR will furnish complete classification guidance for the service to be performed.

l. SCI furnished in support of this contract remains the property of the DoD department, agency, or command that releases it. Upon completion or cancellation of the contract, all SCI furnished will be returned to the direct custody if the responsible security officer designated above. See DoD 5105.21-M-1 for complete guidance of handling SCI.

m. The contractor and COR/TM will revalidate all SCI requirements under this contract with the JSSO INDUSEC annually or when a revised DD Form 254 issued, whichever is sooner.

n. All SCI visit requests by contractors shall be forwarded to the COR/TM for approval and need-to-know certification before being sent through the DIA SSO to the facility to be visited.

Remove paragraph below if SCI will only be accessed at government location.
o. STU-III or STE terminals installed at the contractor's facilities shall be supported by a COMSEC account. STU-IIIs in SCI Facilities (SCIFs) require Class VI Cryptographic Ignition Key (CIK).

(DoD 5105.21, Chapter 3 & Chapter 5)

☐ **Reference Item 10e(2) (Non SCI Intelligence)**.

a. The Joint Staff is required to abide by several security directives, one of which is Director of Central Intelligence Directive 6/6 (DCID 6/6), Security Controls on the Dissemination of Intelligence Information. The following are definitions from that directive.

.

1. Intelligence Community: U.S. Government agencies and organizations identified in Section 3 of the National Security Act of 1947, as amended. DIA is a designated member of the intelligence community.

2. Intelligence Information: Intelligence information and related material include the following information, whether written or in any other medium, classified pursuant to E.O. 13526 or any predecessor or successor Executive Order:

(a) Foreign intelligence and counter intelligence defined in the National Security Act of 1947, as amended, and in Executive Order 12333.

(b) Information describing U.S. 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 U.S. intelligence collection efforts; and

(c) Information on intelligence community protective security programs, e.g. personnel, physical, technical, and information security.

b. Strict adherence to the need-to-know principle for intelligence information applies. Access to intelligence information requires a FINAL U.S. Government clearance at the appropriate level. SCI access by contractor personnel must be approved in writing by the CO/COR/COTR via justification letter. The Contracting Officer's Representative will ensure access is granted to the minimum number of employees required on the strictest need-to-know basis.

c. Violations of the foregoing restrictions that result in unauthorized disclosure of intelligence information shall be immediately reported to the Joint Staff Security Office and DIA.

e. Contractor generated or Government furnished material may not 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 Instruction 5230.24.'**

e. Classified material received or generated under this contract is not releasable to foreign nationals. Public release of classified information is not authorized.

	k. The JS COR will furnish complete classification guidance for the service to be performed. **(DoDI 5220.22 NISP**
☐	**Reference Item 10f (SAP).** a. To execute this contract, security requirements outlined in DoD Directive 5205.7, DOD Instruction 5205.11, Intelligence Community Directive (ICD) 704, ICD 705 and DODM 5205.07 SAP Security Manual Volumes 1-4 will be required. The contractor shall comply with the security provisions of these policies in addition to individual Program Security Guidance. Marking and/or classification guidance for material originated or generated under this contract will be provided through the Special Access Program, Program Manager, under separate cover. Any material generated by the contractor (including correspondence, drawings, models, mockups, photographs, schematics, progress, special and inspection reports, engineering notes, computations and training aids) shall be classified according to content. b. This contract will be performed in a facility approved through the SAP Cognizant Security Authority (CSA) in accordance with applicable SAP security requirements. c. All personnel requiring access to SAP information: (1) Must be U.S. citizen, (2) Have been granted a final TOP SECRET or SECRET (based on classification of SAP) U.S. Government security clearance, (3) Have been approved as meeting ICD 704 criteria by a Government cognizant authority, and (4) Have been indoctrinated for the applicable SAP prior to being given access to any information generated or received under this contract. (5) Immigrant aliens, foreign nationals, or personnel cleared on an interim basis are not eligible for access to classified information released or generated under this contract. (6) Contractor generated or Government furnished property may not be provided to the Defense Technical Information Center (DTIC). d. The Contractor Special Security Officers shall coordinate with JSSO INDUSEC and JS SAP Central Office (JS SAPCO) prior to subcontracting any portion of this contract. **DODM 5205.07 Vols 1-4** a. Contractor employees associated with this contract shall sign appropriate Government non-disclosure statements prior to beginning work. b. All SAP classified material pursuant to this contract shall be protected in accordance with DODM 5205.07 SAP Security Manual Vols 1-4, CJCSI 5250.01 Series, and the appropriate SAP Program Security Plan (PSP) and Security Classification Guide (SCG). c. Any material generated by the contractor (including correspondence, drawings, models, mockups, photographs, schematics, progress, special and inspection reports, engineering notes, computations and training aids) shall be classified according to content. Contractor generated or Government furnished material may not be provided to the Defense Technical Information Center. Contractor generated reports will bear the statement: “Not Releasable to the Defense Technical Information Center” per DoD Instruction 5230.24. d. Guidance for classification shall be derived from the applicable Security Classification Guides, documents, or special instructions. Such material shall not contain contractor logos or similar

	identifiers which identify the specific contractor or team members. Marking and/or classification guidance for material originated or generated under this contract will be provided through the JS SAPCO under separate cover. e. All SAP material remains the property of the releasing Government Cognizant Agency. Upon completion or cancellation of this contract, SAP material previously furnished will be returned to the direct custody of the JS SAPCO or other SAPCO as determined by the Director, JS SAPCO. f. All work with SAP material/computer systems will normally be conducted in government SAP Facilities approved by the Director, JS SAPCO. Any SAP activities conducted at other facilities will require specific, case-by-case approval of Director, JS SAPCO. Access to government furnished computer systems requires compliance with all applicable DoD and JS directives and completion of annual Information Assurance training. g. All SAP access requests in support of this contract will be made through the JS SAPCO. Personnel will meet access eligibility requirements specified in DoDD 5205.07 Vol 2 and CJCSI 5250.01 Series. No access will be granted for SAP information until completion of applicable PAR and PIA in accordance with DoDD 5205.07 Vol 2 and DoDI 5205.11. Personnel desiring access to SAP information must also consent to random Counter-intelligence polygraphs. h. Upon expiration of this contract, the contractor is required to have a close-out inspection by the JS SAPCO to ensure proper disposition of SAP material and equipment. The contractor may be directed to properly destroy the material or return it. No SAP project material is to be retained by the contractor – if applicable; every effort should be taken to transfer it to a follow-on contract or similar effort. This must be done, however, with the contracting officer's (KO) approval.
☐	**Reference Item 10g (NATO)**. Access up to and including [highest level needed] material will be required for reference at [add facility].
☐	All [on-site contractor personnel or contractor personnel] may require access to North Atlantic Treaty Organization (NATO) Secret information for reference only at Joint Staff and/or only to access the Joint Staff Network (JSIN). Access to NATO information will be authorized at the Government location specified in Item 8a. This also means information belonging to, and circulated by, NATO. Special briefings are required for access to NATO. Prior approval of the contracting activity is required for subcontracting. Access to classified NATO information requires a final U.S. Government clearance at the appropriate level and special briefings. Contractor shall be briefed into and debriefed by Facility Security Officer prior to arrival and departure from this contracting effort. If contractor is read into ATOMAL or COSMIC, an annual re-brief is required.
☐	Off-site contractors or subcontractors will not have access to NATO at their facility.
☐	**Reference Item 10h (Foreign Government Information).** a. Access to this information, classified or unclassified is restricted to U.S. citizens. This information includes any Foreign Government Information except NATO. Prior approval of the Joint Staff CO/COR/COTR is required before subcontracting. Access to classified foreign government information requires a final U.S. Government clearance at the appropriate level. Access will be granted on a case-by-case basis at the Government locations specified in item 8a. b. Foreign Government information will be stored and access controlled in the same manner as U.S. Government material of the same classification. **DoD 5105.21-M-1, Chapter 3**

☐ **Reference Item 10i Alternative Compensatory Control Measures (ACCM)**

ACCM Access Required.
REQUIRED FOR ON-SITE ONLY
Individuals working with ACCM will be required to have additional training on the handling and safeguarding of ACCM material and shall comply with the following:

1. All ACCM work will be done "onsite" at the government facility. No ACCM material will be stored/transferred/viewed at the contractor facility.

2. The contractor will safeguard all ACCM information in accordance with CJCSM 3213.02 Series, "Joint Staff Alternative Compensatory Control Measures(ACCM) Program Management Manual Program" and the Program Security Plan (PSP) for the specific program(s):

REQUIRED FOR OFF-SITE ONLY

Individuals working with ACCM will be required to have additional training on the handling and safeguarding of ACCM material and shall comply with the following:

1. All ACCM work will be done in a government-approved facility. Approval shall be granted by appropriate Control Officer.

2. The contractor will safeguard all ACCM information in accordance with CJCSM 3213.02 Series, "Joint Staff Alternative Compensatory Control Measures (ACCM) and the Program Security Plan (PSP) for the specific program(s):

3. Joint Staff Alternative Compensatory Control Measures (ACCM) and the Program Security Plan (PSP) for the specific program(s) the contractor has been briefed to:

    - The Control Officer will coordinate identification of the authorized users for each ACCM program processed by the contractor. Access to the ACCM information shall be limited to only those with a specific association with operational task, mission, or specific contract deliverable.

    - A list of authorized users shall be maintained as an Access Control List (ACL), which will define the individuals or groups, granted access to ACCM information. A record of each ACL, and any changes, shall be maintained during the duration of the contractor's involvement in the ACCM and will be filed with the government ACCM PCO when the contract is terminated.

    - Systems processing ACCM information must provide NTK enforcement based on a Discretionary Access Control (DAC) policy that establishes a security structure that defines and controls access between users and objects (e.g., data/information, files, and programs) in the system. Use of a single "group" ID with a single password is not authorized for control of access to ACCM information) The ACCM PCO shall control and verify the establishment and function of DACs on the contractor's information system before it is used to process ACCM information.

☒ **Reference Item 10j Controlled Unclassified Information (CUI)**

(Do not select this item unless the contract requiring access to classified information also includes a requirement for access to CUI, in accordance with GCA specific classification guidance. Safeguards, and procedures necessary for the protection of any CUI required in the performance of this specific classified contract.)

If box is checked, Contractor personnel are required to complete the "DoD Mandatory Controlled Unclassified Information (CUI)" course JS-US082 in JKO as part of DoD's CUI implementation plan. The course provides information on the eleven training requirements for identifying, marking, accessing, safeguarding, decontrolling, and destruction of CUI.

	Course can be accessed directly at https://jkosupport.jten.mil/html/COI.xhtml?course_prefix=JS&course_number=-US082. Contract personnel are expected to complete the training in accordance with contract requirements. DOD INSTRUCTION 5200.48 CONTROLLED UNCLASSIFIED INFORMATION (CUI)
☒	**Reference Item 10k OTHER.**
☐	**NC2-ESI Access Required.** a) This contract requires that specified contractor employees be granted access to Nuclear Command and Control - Extremely Sensitive Information (NC2-ESI). NC2-ESI material remains under US Government control at all times. Access to NC2-ESI by contractor personnel will be limited to US Government facilities. b) In order to be considered for access to NC2-ESI, applicant must be a United States citizen. In addition, applicant must have a Top Secret clearance based on a favorable Single Scope Background Investigation (SSBI) completed within the past five years. No waivers will be considered. **Employees requiring NC2-ESI access will be processed as follows:** 1. The Contractor will nominate personnel to the COR/TOM/TIM. Contractor will nominate only technically qualified personnel who meet citizenship requirements stated above. 2. The COR/TOM/TIM will prepare the memorandum, which includes temporary access roster and a copy(s) of the security clearance records from the Joint Adjudication Personnel System, and forward the request to the J-39 a request memo to process certain contractors for NC2-ESI access. The request will be marked with the appropriate markings (i.e., FOUO, Privacy Act Protected, etc.) and/or classification as may be required per the security classification guide. This request will contain the following for each individual: a. Contractor Name b. Contractor Social Security Number c. Company name, address, CAGE code, telephone number d. Date and place of birth e. Citizenship of employee. f. Citizenship of employee’s spouse. g. NC2-ESI Category required. h. Employee's clearance level and date, investigation type and date. i. Inclusive dates NC2 access will be required. j. Contract number. k. Contract period of performance end date (expiration date) l. Descriptions of the applicant’s duties under the contract that will require access to NCS-ESI m. Justification for requesting NC2-ESI accesses (include referring Joint Chiefs of Staff (JCS) office or JCS POC). n. POC for Memorandum, telephone number

	3. If the applicant meets the clearance and investigation criteria, nomination must be received by J-39 and must be received 60 days prior to anticipated date NC2-ESI access is required. 4. If the applicant does not meet the clearance/investigation criteria, nomination must be received six months before anticipated date NC2-ESI access is required. 5. When temporary access to NC2-ESI has been approved by the J-39, the COR will notify the employee(s) of scheduled brief date. 6. NC2-ESI access will require briefing and debriefing to be accomplished by J-39. Contractor will cooperate with J-39 in making personnel available with sufficient lead-time to permit J-39 to arrange for required briefings and debriefings. 7. Contractor will advise J-39 of any adverse information or change in status of an employee who has been granted access to NC2-ESI, i.e., marriage, divorce, or remarriage. 8. The COR is responsible for notifying the J-39 when the employee is transferred from one facility to another within the company, when the employee's employment is terminated, when they resign, or have been transferred and do not require continued access. 9. The FSO is responsible for ensuring that the employees complete the required security forms for submission to DSS Facility Security Branch in a timely manner. 10. Information that an individual has been granted access to NC2-ESI is unclassified.
☒	**Performance in Government Facilities.** This contract requires personnel to perform work as a member of, or in direct support of, the Joint Staff and will require individuals to work within Government controlled facilities. **A. In and Out Processing.** This contract requires personnel to perform work as a member of, or in direct support of, the Joint Staff and will require individuals to obtain and maintain government issued building access cards to enable performance within Government controlled facilities. As such, all contractor personnel are required to in-process with the Joint Staff Security Office or location SSO prior to reporting for work. As a condition of this contract, all personnel issued government access cards are required to ensure the card is returned to the Joint Staff Security Office upon removal from the contract or termination of employment under this contract. Applies in all cases were performance in a government facility is applicable. **B. Common Access Cards (CAC).** This contract requires personnel to obtain the Government issued Common Access Card (CAC) in order to access government computer systems. As such, all contractor personnel are required have an approved Form 8 or exception to policy letter before a CAC Request will be approved in the Contractor Verification System (CVS) by a JSSO Trusted Agent (TA). The COR will submit the request to JSSO INDUSEC for approval. As a condition of this contract, all personnel issued Government CACs are required to ensure the card is returned to JSSO upon removal from the contract or termination of employment under this contract. **C. NIPRNET access required.** This contract requires the contractor to access and use the unclassified government computer system known as the NIPRNET at locations identified by the government customer. All provisions of the DoD Information Assurance Certification and Accreditation Process (DIACAP) apply. This system is Unclassified only, and inappropriate or improper use of the system will result in a reportable incident to Defense Security Service (DSS). **D. SIPRNET access required.** This contract requires the contractor to access and use the classified government system known as the SIPRNET at locations identified by the government customer. All provisions of the DoD Information Assurance Certification and Accreditation Process (DIACAP) apply. This system is authorized for use to but not exceeding the SECRET level only, and inappropriate or improper use of the system will result in a reportable incident to Defense Security Service (DSS).

	E. JWICS access required. This contract requires the contractor to access and use the classified government system known as JWICS at locations identified by the government customer. This system is authorized for use to but not exceeding the TS-SCI level only, and inappropriate or improper use of the system will result in a reportable incident to Defense Intelligence Agency (DIA) **F. TRAINING REQUIREMENTS:** a. **OPSEC TRAINING:** Contractor shall abide by OPSEC policies and procedures, as detailed in CJSCI 3213.01C and as directed by the OPSEC Manager or an OPSEC representative. Contractor shall accomplish their initial OPSEC training within 90 days of in-processing and complete annual OPSEC training. Contractor shall notify their OPSEC Coordinator or an OPSEC representative of recommendations for the OPSEC program or potential OPSEC concerns. POC: JSSO OPSEC (703-571-9959) **b. IA TRAINING:** Contractor shall abide by IA policies and procedures, as detailed in JSI 5210.01 and as directed by the Information Assurance Manager (IAM) or an IA representative. POC: JSSO IA (703-517-9956)
☒	**Reference Item 11a. (Have Access to Classified Information Only at another Contractor's Facility or Government Activity):** Performance of the classified portion of this contract is restricted to Joint Staff facilities and/or the locations cited in Block 8a, above. The Joint Staff CO/COR/COTR will provide security classification guidance for performance of this contract. SCI and collateral classified information may be processed, displayed, discussed or stored at Joint Staff facilities and the contractor's facility, provided the activity takes place in an appropriate area accredited and/or approved by an U.S. Government agency.
☐	**Reference Item 11b Receive Classified Documents Only. REQUIRED FOR OFFSITE ONLY** Any classified information generated in performance of this contract shall be classified according to the markings on the source material. All classified information received is the property of the U.S. Government/Joint Staff. The Joint Staff CO/COR/COTR will be contacted at the expiration or termination of this contract for proper disposition instructions.
☐	**Reference Item 11c. Receive and Generate Classified Material. REQUIRED FOR OFFSITE ONLY** **a. The Contractor may receive and generate classified information material up to and including TOP SECRET/SCI - enter appropriate level.** b. If the contractor/subcontractor is required to process classified information on an Automated Information System/Network (AIS/N) at the contractor/subcontractor's facility, the information must be processed on an AIS/N accredited by a U.S. Government agency, and the contractor/subcontractor will be required to maintain/store the AIS/N in a U.S. Government accredited area, as appropriate. c. Joint Staff contractors processing collateral classified information on contractor AIS equipment/networks within facilities accredited by the Defense Security Services will be accredited in accordance with DoDI 5220.22 NISP. Contractor AIS equipment/networks used to process SCI information will be accredited in accordance with ICD 503, regardless of location. **Prior to processing SCI information on a Contractor AIS System/Network, the AIS System/Network must be accredited by DIA. (Contractors must contact the Joint Staff Security Office to initiate the SCI accreditation process for an AIS System/Network or a SCIF.)** Note that if 11c is marked then 1b must have a level of storage at contractor's facility.
☐	**Reference Item 11d. Fabricate, Modify, or Store Classified Hardware. REQUIRED FOR OFFSITE ONLY**

	a. The Contractor may fabricate, modify or store classified hardware up to and including TOP SECRET/SCI - enter appropriate level using JS/DIA approved safes, vaults or security containers. b. Equipment used to fabricate or modify classified information must be secured IAW applicable DoD Instructions and DoD 5105.21-M-1. c. Unless directed in writing otherwise, all classified information and/or material received or generated by the Contractor (including classified waste material) must be returned to the Joint Staff, unless retention is requested for a specific period of time and authorized in writing by the JS CO/COR/COTR. At the termination or expiration of this contract, the JS CO/COR/COTR will be contacted for proper disposition instructions. d. SCI material/hardware will ONLY be stored in a SCIF, with a current SCI accreditation. **DoD 5105.21-M-1, Chapter 3**
☐	**Reference Item 11e. Perform Services Only.** Contractor is performing a service only and is not expected to produce a deliverable item. **For Graphic Arts Services:** Contract is for Reproduction Services only. The highest level of classification for this contract is ***(insert level)*.** Classification markings on the material to be reproduced will provide the classification guidance necessary for the performance of this contract. **For Engineering Services**: Contract is for engineering services. Classification and markings on the material to be furnished will provide the classification guidance necessary for performance of this contract. **For Equipment/Janitorial Maintenance Services:** Contract is for equipment/janitorial maintenance services on equipment, which processes classified information. Actual knowledge, generation or production of classified information is not required for performance of this contract. Cleared personnel are required to perform this service for proximity access to classified information and because physical security measures cannot be employed to prevent or preclude visual and/or aural access to classified information. **For Guard Services:** Contract is for Guard Services. Cleared personnel are required to perform this service.
☐	**Reference Item 11f. Have Access to U.S. Classified Information Outside the US, Puerto Rico, US Possessions and Trust Territories.** The contractor may require access to classified information at one or more Foreign Government Sites and/or U.S. Government facilities OCONUS (Outside the Continental United States). The government program manager will provide travel orders and direction prior to departure. Contract performance will occur at the following U.S. activities: a. City/Country Contractors when performing or traveling outside the United States under this contract will: a. All personnel will obtain an AOR specific foreign travel brief within 90 days of travel and will provide proof of training to the COR/CM. b. All personnel will receive the Antiterrorism Level I Awareness training within one year prior to travel. c. The contractor may only have access to U.S. classified information outside the U.S. if they are traveling under JS government orders.
☐	**Reference Item 11g. Be Authorized to Use the Services of the Defense Technical Information Center (DTIC) or Other Secondary Distribution Center.** Contractor generated or Government furnished material may not be provided to the Defense Technical Information Center (DTIC). The contractor must prepare and forward DD Forms 1540 to the Joint Staff CO/COR/COTR for authorization BEFORE the services may be requested.

	Technical information on file at the Defense Technical Information Center (DTIC) will be made available to the contractor if the contractor requires such information. The Joint Staff CO/COR/COTR will certify the field of interest relating to the contract. The Joint Staff CO/COR/COTR will submit on behalf of the contractor. For subcontractors, the prime contractor submits the DD 1540 with the Joint Staff CO/COR/COTR verifying need to know. The contract may also submit DD Form 2345 “Military Critical Technical Data Agreement” (after registration with DTIC) to the Defense Logistic Services for access to unclassified, military critical technical data from other DoD sources. The Joint Staff CO/COR/COTR must certify the need-to-know-to DTIC. Special access information will not be sent to the National Defense Technical Information Center or the U.S. Department of Energy of Scientific and Technical Information. **(DoDI 5220.22 NISP, Chapter 11)**
☐	**Reference Item 11h. Require a COMSEC Account.** a. The contractor is authorized to receive Government furnished cryptographic equipment/material. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level and a briefing detailing proper safeguarding of COMSEC material/information. Further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior approval of the contracting activity. Contractor must forward request for COMSEC material/information through government program manager to COMSEC Custodian. Contractor is responsible for accountable COMSEC information and must provide a complete inventory as required by COMSEC account manager. b. STU-III terminals installed at the contractor's facilities shall be supported by a COMSEC account through the CSO. STU-IIIs in the SCI Facilities (SCIFs) require Class VI Cryptographic Ignition Key (CIK). c. Public release of COMSEC information/material is not authorized.
☐	**Reference Item 11i. Have TEMPEST Requirements (aka Emissions Security).** **REQUIRED FOR OFFSITE ONLY** For Collateral level classified processing enter: To determine possible TEMPEST countermeasures the contractor will assist in the vulnerability evaluation. The Joint Staff requires the contractor to provide a list and layout of equipment, the estimated percentage of classified information processed, cable/conduit runs, a floor plan layout that depicts placement of equipment in relation to other rooms, equipment distances from walls or uncontrolled areas, and physical security being afforded the equipment both during processing and after hours. Drawings/maps showing location of facility in relation to surrounding buildings/structures and any other information necessary to determine the tempest countermeasure requirements are needed. For SCI and/or SAP level classified processing enter: The contractor will not process classified information by electrical means prior to a TEMPEST evaluation of the equipment/systems and facility, and written CSA certification that the facility meets SCI/SAP TEMPEST criteria. In order to expedite the TEMPEST evaluation, the contractor shall provide a list and layout of equipment in accordance with DoD 5105.21-M-1, Appendix J. The enclosure will include a floor plan layout that depicts placement of equipment in relation to other equipment, telephone lines and instruments, cable/conduit runs, etc. The drawing(s) are to show dimensions of rooms, physical relation to other rooms, equipment distances from walls or controlled areas, and physical security being afforded the equipment both during processing and after hours. The approval must be for processing information of the same or higher-level security classification and for the same facility and items of equipment. Drawings/maps showing location of facility in relation to surrounding buildings/structures and any other information necessary to determine the tempest countermeasure requirements are needed. The contractor is required to impose TEMPEST countermeasures on information processing equipment after vulnerability assessments are completed. Work must be performed in an accredited SCIF. Prime contractors may not impose TEMPEST requirements on their subcontractors without GCA approval. The contractor shall not process classified information by electrical means prior to coordination with the DIA Certified TEMPEST Testing Authority (CTTA) (out of DIA: DAC-2A). The DIA CTTA is the only authorized approving agent for

	TEMPEST systems within JS. The above TEMPEST evaluation and DIA approval will not be required if previous DIA approval can be furnished and is no more than 2 years old. The existing approval must be for processing information at the same or higher level and at the same facility and items of equipment. If requested by the DIA CTTA, TEMPEST Countermeasure Assessment Request may be included as an attachment to the DD 254. [The contractor shall ensure that emissions security (EMSEC) conditions related to this contract are minimized.] **DoD 5105.21, Vols 1-3**
☒	**Reference Item 11j. Have Operations Security (OPSEC) Requirements.** a. The contractor will comply with Operations Security (OPSEC) requirements contained in the contract, addendum thereto, or identified herein. b. The contractor will take the necessary precautions to ensure employees who require access are instructed on OPSEC and the protection of sensitive, unclassified information as well as Critical Unclassified Information (CUI). c. The contractor will need to be familiar with OPSEC and be required to take mandatory OPSEC training. d. The contractor will take the necessary precautions to ensure employees with access to the sensitive and critical information are instructed not to disclose or disseminate any information relating to the conduct and performance of the contract to any individual not authorized to perform on this contract. e. The Contractor will ensure all UNCLASSIFIED, SENSITIVE AND CRITICAL information is returned to the Joint Staff and not destroyed. f. Further OPSEC guidance may be obtained by contacting the Joint Staff OPSEC division at 571-9959 or the Directorate Security Managers for this program. g. OPSEC and other security guidance issued to the prime contractor will also apply to subcontractors working on this effort.
☐	**Reference Item 11k. Authorized to use Defense Courier Service.** This contract may require the use of the Defense Courier Service (DCS) for shipment of classified information/material. The prime contractor must obtain written approval from NGA CO/COR/COTR and provide the approval to the Commander, Defense Courier Service, Attn: Operations Division, Fort George G. Meade, MD 20755-5370. Only certain classified information qualifies for shipment by DCS. The Contractor must obtain guidance concerning shipment of classified information/material from the DCS. Prior approval of NGA CO/COR/COTR is required before a prime contractor can authorize their subcontractor to use the services of DCS. Off-Site: Contracting activity will request DCS Services from the Commander, Defense Courier Service, ATTN: Operations Division, Bldg 9-830, Fort George G. Meade, MD 20755-5370. On-Site: Route all requests through Government Activity Office via Top Secret Control Officer (TSCO). Route all requests for SCI access through DIA SSO. Prior approval of the contracting activity is required before granting subcontractor use of DCS services.
☒	**Reference Item 11l. Controlled Unclassified Information (CUI)** Do not select this item for a contract that only requires receipt, storage, or generation of CUI. Check this item if item 10.j. is checked and one of the other items (11a., 11b., 11c. or 11d.) is checked that specifically indicates that this contract requires access to classified information for performance. Item 22.l. and Item 10.j. only pertain for the protection of any CUI required in the performance of this specific classified contract. DOD INSTRUCTION 5200.48 CONTROLLED UNCLASSIFIED INFORMATION (CUI)

☒ **Reference Item 11m. Other.**

a. When portions of this work under this contract occur at JS facilities, all JS policy and contractor personnel shall adhere to procedures that relate to security management. In the event that the development of information or material is not clearly covered by the contract or JS security policy and procedures, the contractor is required to seek JS guidance regarding its handling**. Portions of this effort may require working at undisclosed locations or facilities not publicly acknowledged. The contractor will not display/advertise JS products while working at these facilities.** Any questions the contractor or contractor personnel may have on the applicability of these security requirements shall be addressed to the Joint Staff CO/COR/COTR and/or the Joint Staff Security Office.

b. Contractors shall provide all cleared employees with security training and briefings commensurate with their involvement with classified information. The contractor shall provide all cleared employees with some form of security education and training at least annually. Refresher training shall reinforce the information provided during the initial security briefing and shall keep cleared employees informed of appropriate changes in security regulations. Contractors shall maintain records about the programs offered and employee participation in them. Contractors may obtain defensive security, threat awareness, and other education and training information and material from their CSA or other sources.

DoD 5105.21, Vol 3

c. Only contractor/subcontractor/consultant personnel properly nominated by the contractor and approved by the Joint Staff CO/COR/COTR are authorized to perform on this contract and have access to classified information/material.

d. Prior to performance on any Joint Staff contract in which the contractor will have access to a U.S. Government/Joint Staff AIS System/Network (ie, JSIN), the contractor must have received the briefing/training required by JSM 5210.01B, "Information Assurance Management Program."

e. The contractor shall safeguard information IAW DTM 08-027, Security of Unclassified DoD Information on Non-DOD Information Systems. Do not post unclassified FOUO DoD information that has not been cleared for public release to website pages that are publicly available. Access controls must be restricted by user identification or password, user certificates, or other technical means and provide protection via use of TLS/SSL 6.0.

f. The contractor will ensure all Government computer accounts, assigned to contractor personnel during the performance of this contract, are deleted/disabled **within 24 hours** of completion, termination, removal, reassignment or other departure from the contract. **(NOTE: Either the contractor, contractor's supervisor, or the Joint Staff CO/COR/COTR, may disable the contractor's AIS system/network account(s) by submitting an OCIO Form 150 with the contractor's name, date of the contractor's departure, and identity of any AIS system/network accounts in which the contractor had access) through their Directorate Security Manager or MILSEC.** In either instance (i.e., cessation of contract or cessation of contractor personnel with this contract), the contractor shall notify the Joint Staff CO/COR/COTR in writing of all government computer accounts assigned to contractor personnel during the performance of this contract are deleted in accordance with this provision.

g. In performance of this contract, contractor/subcontractor /consultant will ensure any software to be provided or returned, under this contract, will be free from computer virus'

which could damage, destroy, or maliciously alter software, firmware, or hardware, or which could reveal to unauthorized persons any data or other information accessed through or processed by the software.

h. The CO/COR will notify the Joint Staff (Industrial Security Branch, 703-693-9699 of all contractors who have departed or are no longer performing on the contract, and the date they were debriefed and by whom.

i. The contractor will report any adverse information coming to their attention to the Joint Staff Security Office, Personnel Security Branch. (The subsequent termination of employment of an employee does not obviate the requirement to submit the report.)

j. In performance of this contract, the contractor may be required and is authorized to hand carry or courier classified information up to an including TOP SECRET/SCI - enter appropriate level and Locations. As such, contractor personnel are required to contact their Directorate Security Manager to obtain courier cards. Instructions for obtaining the courier card must be provided by COR and must be adhered to in order to obtain a courier card. The contractor/subcontractor will comply with the appropriate Joint Staff/DIA and DoD guidance for hand carry/courier of classified information.

k. In performance of this contract, the contractor will take the necessary precautions to ensure contractor/subcontractor employees out-process with the Joint Staff Security Office of the local site SSO upon termination/completion of this contract; The contractor will ensure contractor/subcontractor return any property/equipment (i.e., badge, common access cards (CAC), alternate tokens, vehicle hang tag, courier authorization, keys, etc.) issued by the Joint Staff. **In addition, when a contractor employee is reassigned, transferred, terminated or is no longer required to perform on this contract, the contractor FSO/CSSO will immediately notify the Joint Staff CO/COR/COTR, in writing, to cancel that employee's visit authorization.**

l. All prime contractors working the Joint Staff acquisition vehicles (RFI/RFP/SOWs/DD 254s, etc.) will identify subcontractors, and have these vendors vetted with Joint Staff Industrial Security Office for Key Management Personnel (KMP), Foreign Ownership, Controlling Interest (FOCI), and other CFIUS (Committee for Foreign Investment in the United States) related issues or concerns. Contact the Joint Staff Industrial Security Office at 703-693-9699)

m. The contractor is not authorized to destroy classified materials.

n. All visit access requests (VARs) by contractors, who will not sit in on-site JS spaces, shall be sent via the Defense Information Security System (DISS) to JSSO (Collateral SMO: DJJ0212) or appropriate SMO for the effort by the contractor’s Facility Security Officer (FSO). The COR/TOM must approve the VAR prior to sending the request to the facility being visited. Contractors must also provide a copy of the VAR to the security manager.

o. If the contractor is currently in SCI Status and position has a need-to-know, a perm cert must be sent via DISS to DDJ0212.

p. **“Spillage” Provision Language**

"Negligent Discharge of Classified Information (NDCI). When information is placed on or processed on an information system with insufficient security controls to appropriately protect it (e.g., classified data on an unclassified system) there is a potential for an unauthorized disclosure. Such actions will be classified as a security violation, specifically a negligent discharge of classified information or NDCI. Contractors that cause NDCIs during the course of the contract shall be held financially liable for all actual accumulated restoration costs incurred, as described below, but not less than $5,000 per incident. Such costs will be deducted from the contract price, and are not reimbursable.

a. Restoration costs above $5,000 will be itemized. DISA has developed a Classified Message Incident Standard Operating Procedures (SOP) that will be followed in the event of an NDCI by the Contractor. Personally Identifiable Information (PII) incidents fall under this category. This is not an exclusive remedy (e.g., in the case of PII spillage, identity theft or other insurance may be needed to protect the individuals).
b. NDCI Cleanup actions may include the following actions:
   i. Server destruction
   ii. Hard drive wipe and destruction
   iii. Containment actions"

(References: 1. CJCS Directive: dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf. 2 In accordance with (IAW) Department of Defense Directive (DODD) 8500.01E, ... Spillage of Classified ... accomplished IAW CJCSI 6211.02, "Defense Information ...

2. DODD 8500.01E: Cybersecurity dtic.mil/whs/directives/corres/pdf/850001_2014.pdf Department of Defense . INSTRUCTION . NUMBER 8500.01 . March 14, 2014 . ... DoD Directive 3020.26, "Department of Defense Continuity Programs," January 9, 2009.

3. Definitions and refs: www.nsa.gov/ia/_files/factsheets/Final_Data_Spill.pdf Securing Data and Handling Spillage Events The Information Assurance Mission at NSA, What Is a Data Spill and Why Is It a Problem? Loss of control over sensitive and ...

4. DoD Man 5200.01 Protection of Classified Info dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf . Department of Defense . MANUAL NUMBER 5200.01, Volume 3 . February 24, 2012 . Incorporating Change 2, March 19, 2013 . ... Classified Information Spillage

5. Article on reducing leaks by improving info assurance standards: http://www.titus.com/titus-blog/2010/09/reducing-the-costs-of-classified-information-spillage-by-improving-data-classification-processes/) As described it gives notice of reasonably anticipated damages, so Liquidated Damages under FAR 11.500 need not be considered.)

REQUIRED FOR SCI ONLY

q. Prospective contractor employees shall submit a completed to the DD Form 1157 to Servicing SSO or, if onsite, a SCI Request Requirements Packet to Joint Staff Security Office, Personnel Security Division, no less than 30 days before the starting date of the contract or 30 days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee or vendor.

r. The COR or COTR is responsible for notifying the contracting company that the employee is eligible for SCI and can start working on the contract, or that the employee was denied SCI eligibility, and is ineligible for contract performance.

NOTE: Joint Staff Security Office, Personnel Security Branch, will not be responsible for due process for contractors not meeting SCI criteria

s. This contract may involve handling and storage of classified material. Contractor has responsibility for alarmed areas (except SCI facilities approved by JSSO) and properly escorting both contractor and government visitors (except SCI facilities approved by JSSO). Contractor is directly accountable for security actions and government rule compliance to include COMSEC and OPSEC requirements. Contractors will be subject to investigation and potential adverse actions in the event of security deviations and violations.

t. In addition, in performance of this contract, the contractor/subcontractor will comply with security guidance provided by the Joint Staff CO/COR/COTR and/or contained in the following directives. NOTE: The Unclassified directives listed below can be downloaded via the Web site **www.dtic.mil/whs/directives**. **Other directives, classification and marking guides should be obtained through the Joint Staff CO/COR/COTR:**

The following highlighted instructions/manuals supersede previous versions and are applicable as of December 10, 2021:
32 CFR Part 117, NISPOM Rule §117.21
DoDI 5220.22, Incorporating Change 3
DoDM 5220.32, Vol 1, Industrial Security Procedures for Government Activities, Change 2
DoDM 5220.32, Vol 2, National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI),Change 2

DoDM 5200.1, Information Security Manual 1 Mar 12(Incorporating Change 1, May 4, 2018)
DODI 5200.48, Controlled Unclassified Information, 6 Mar 2020
DoDM 5200.02, Procedures for DoD Personnel Security Program, April 3, 2017
DoD 5105.21 Vols 1-3, Sensitive Compartmented Information Administrative Security Manual, Oct 12, Vol 1, Ch 1, 16 May 2018; Vol 2, Ch 1, 5 Apr 2018; Vol 3, Ch 1, 5 Apr 2018
DoD C-5230.23, Intelligence Disclosure Policy, 18 Nov 83
DoD 8500.01E Information Assurance Oct 02
DoD Special Access Program (SAP) Security Manual: General Procedures Number 5205.7 Vol. 1 June 18 2015, Incorporating Change effective February 12, 2018
ICD 503, Sep 2008
ICD 703, Jun 2013DCID 6/7, Intelligence Disclosure Policy, 20 Apr 01
ICD 705, May 2010 and Technical Specifications to ICD 705 v1.4, Sep 2017
ICD 503, Information Technology Systems Security Risk Management, Certification and Accreditation, 15 Sep 08
ICD 701, Security Policy Directive for Unauthorized Disclosure of Classified Information, Dec 2017
ICD 704, Personnel Security Standards and Procedures Governing Eligibility for Access to SCI and Other Controlled Access Program Information, Jun 2018
USSAN Instruction 1-07, Apr 2007
Applicable Program Security Directives (PSDs)
Security Classification Guides (SCGs)
Local Standard Operating Procedures

The Contractor shall comply with the policies and procedures identified in the contract that implement the following:

	Homeland Security Presidential Directive-12 (HSPD-12) Office of Management and Budget (OMB) guidance M-05-24 Federal Information Processing Standards Publication (FIPS PUB) Number 201
☒	**Government Travel.** As required by the Government Program Manager, contactor will be authorized travel/Temporary Duty (TDY) outside the NCR for official government business. The Government Program Manager is responsible for providing travel orders and direction prior to travel.
☐	**IT Operation and Support Positions.** Contract will require access to sensitive [unclassified and/or classified] government automated information systems (AIS) at different levels. The contractor shall identify all IA function requirements (IAM/IAT), as detailed in 8570.01, to be performed by contractors in their statement of work/contract. The contractor shall be appropriately certified and provide the certificates to JSSO. IAT-I, II, and III require at least a SSBI and the following training and user agreements must be signed and on file with JSSO Information Assurance (IA) before access is granted: Privilege User Agreement Normal User Agreement Joint Staff Information Assurance Training All provisions of the DoD 8570.01-M Change 2, "Information Assurance Workforce Improvement Program" dated 20 Apr 10, apply to this contract. Contractor must also comply with the Joint Staff Information Assurance (JS IA) Policy, JSI 5210.01. ☐ **System Engineers or IAT-III access required.** ☐ **System Administrator or IAT-II access required.** ☐ **Network Administrator or IAT-I access required.**
☐	**Perform as Office Security Managers.** Contractor may require performance as alternate Office Security Manager. Responsibilities of the Office Security Manager are contained in the Joint Staff Information Security Manual and must be adhered to.
☐	**Perform as Activity Security Representatives.** Contractor may require performance as alternate Activity Security Representative (ASR). Responsibilities of the ASR are contained in the PWS and must be adhered to.
☒	**Reference Item 12. Public Release:** Public release of classified information is not authorized. Any unclassified information received or generated under this contract intended for public release by the contractor must be submitted to Joint Staff Public Affairs through the Joint Staff CO/COR/COTR for approval prior to public release (It is the responsibility of the Joint Staff CO/COR/COTR to obtain this approval). **(NI 5720.1, DoD, 5105.21 Vol 1-3, Chapter 1 and DoDI 5220.22 NISP)**
☒	**Reference Item 13. Security Guidance:** a. Additional security guidance can be obtained through the Joint Staff CO/COR/COTR or by contacting the Joint Staff Industrial Security Branch Chief at 757 203-7144. b. Inquiries pertaining to the classification guidance will be directed to the Joint Staff CO/COR/COTR for this contract. c. Access to intelligence information requires special briefings and a US Government clearance at appropriate level TS SI/G/TK/HCS. Prior approval of COR is required for subcontracting.
☒	**Reference Item 14. Additional Security Requirements:** a. FOREIGN NATIONALS are **prohibited** from access to any classified information associated with this contract.

	b. Contractor compliance with DoDI 5220.22 NISP, "National Industrial Security Program" Operating Manual, February 2006 is mandatory. **(DoDI 5220.22 NISP)**
☒	**Reference Item #15 (Inspections): DIA has exclusive security responsibility for all SCI classified materials released or developed under this contract. DSS retains responsibility for all non-SCI classified material/information released to the contractor or developed by the contractor under this contract and held within the contractors' collateral facility. DSS is relieved of security inspection responsibility for all classified material/information maintained within the contractor SCI accredited space.** In accordance with DoDI 5220.22 NISP and DoD 5105.21, Vols 1-3, the Joint Staff as a GCA will provide security guidance/assistance as needed, and conduct Customer Assistance Visits to review security aspects of this contract to ensure the protection and safeguarding of classified information. Note: Request DSS provide to the Joint Staff Security Office copies of any security incidents relative to this contract and copies of the latest annual DSS Industrial Security Review report for the contractor's facility, at the below address: Joint Staff Security Office Attn: Industrial Security, Contractor Incident Reporting 9300 Joint Staff Pentagon Washington, DC 20318-9300 **Addendum Updated: 20220712**