U.S. Army Corps of Engineers (USACE)

CONTRACT REQUIREMENTS PACKAGE SECURITY REVIEW COVER SHEET

For use of this form, see the HQ-USACE OPORD 2022-03; the proponent agency is CECO-P.

SECTION I - CONTRACT INFORMATION

1. CONTRACT or REQUIREMENTS TITLE	2. LOCATION
3. SOLICITATION/CONTRACT NO.	4. CLASS APPROVAL REQUEST NUMBER

5. CONTRACT TYPE

☐ Construction ☐ MATOC/SATOC/IDIQ ☐ Service ☐ Supply ☐ Task Order ☐ Other (*specify*) _____

SECTION II - PURPOSE

This form documents the review of the requirements package (e.g., performance work statements (PWS), statements of work (SOW), statements of requirements (SOR)) for antiterrorism (AT) and other related protection matters to include, but not limited to: operation security (OPSEC), information assurance (IA), physical security, law enforcement, intelligence and industrial security. **Army policy** requires all services contracts, and supply contracts above the simplified acquisition level threshold (SAT), to include a signed AT/OPSEC cover sheet; this does not apply to supply contracts below the SAT, field ordering officer actions, or Government Purchase Card purchases. Local policy may require this form for supply contracts under the SAT based on risk and threat. **HQ-USACE policy** mandates that prior to submitting requirements packages to the supporting contracting activity, the Antiterrorism Officer (ATO) and OPSEC Officer for the Requiring Activity (RA) review (including coordination with other staff, as appropriate) each requirements package, unless a signed class approval request form is completed. If the RA does not have an ATO or OPSEC Officer, the first ATO and OPSEC Officer in the chain of command will review the contract for AT/OPSEC considerations. For contracts that involve Information Assurance/ Information Technology (IA/IT) services (e.g., desktop or network services, software or business system development/operations/ maintenance, or management of websites, servers, enterprise databases, etc.), the servicing Information Systems Security Officer (ISSO) or similar IA professional supporting the RA will review the contract for IA/IT considerations and sign this coversheet.

SECTION III - STANDARD CONTRACT LANGUAGE

Reviewers shall consider the applicability of each requirement, and check each block as "Yes" or "N/A." If the standard PWS/SOW/SOR language text found in Section IX of this form is sufficient to meet specific contract requirements, check "Yes" in the corresponding block below, and include this language in the PWS/SOW/SOR. If the standard language applies but additional language is required, check "Yes" and include both the standard language and additional contract specific language in the PWS/SOW/SOR. If standard PWS/SOW/SOR language does not apply, check "N/A."

SECTION IV - REQUIRED CLAUSES

Required Clause(s) (*see Section IX for sample language*)	YES	N/A
1. General security requirements and guidance.	☐	☐
2. AT Level I training.	☐	☐
3. Physical security and access control requirements.	☐	☐
4. Contractor personnel requiring a common access card (CAC).	☐	☐
5. Security requirements for contract performance outside the US.	☐	☐
6. Suspicious Activity Reporting training (e.g. iWATCH, CorpsWatch, or See Something, Say Something).	☐	☐
7. Contract personnel requiring access to Government information systems.	☐	☐
8. Contracts requiring a formal OPSEC program.	☐	☐
9. Training requirements for the protection of sensitive information.	☐	☐
10. Information Assurance/Information Technology requirements.	☐	☐
11. Contracts requiring handling or access to classified information.	☐	☐
12. Threat Awareness Reporting Program.	☐	☐
13. Escorting in classified and/or sensitive areas.	☐	☐
14. Pre-screen candidates using E-Verify Program.	☐	☐
15. Contracts requiring armed security guards.	☐	☐
16. Contracts requiring delivery of food and water.	☐	☐

SECTION V - REMARKS	
1. CONTRACT TITLE	2. LOCATION
(The RA may add general information for the Reviewers below, but must also provide the complete requirements document (e.g., PWS, SOO, etc.)	

SECTION VI - ANTITERRORISM REVIEWER'S SIGNATURE		
I am ATO Level II certified and I have reviewed the requirements package and understand my responsibilities IAW Army Regulation 525-13, Antiterrorism.		
1. TYPED OR PRINTED NAME	2. RANK/CIVILIAN GRADE	3. PHONE NUMBER
4. SIGNATURE	5. DATE	

SECTION VII - OPERATIONS SECURITY REVIEWER'S SIGNATURE		
I am OPSEC Level II certified and have reviewed the requirements package to ensure that there are no OPSEC concerns regarding the release and/or publication of attached documentation to public forums as well as to determine OPSEC requirements for the Contractor, and understand my responsibilities IAW Army Regulation 530-1, Operations Security.		
1. TYPED OR PRINTED NAME	2. RANK/CIVILIAN GRADE	3. PHONE NUMBER
4. SIGNATURE	5. DATE	

SECTION VIII - INFORMATION ASSURANCE REVIEWER'S SIGNATURE (*Required only if block 10 is checked "Yes."*)		
I am certified at the appropriate Information Assurance Technology (IAT) and/or Information Assurance Management (IAM) level based on DoD 8570.01-M; I have reviewed the requirements package and understand my responsibilities in accordance with AR 25-2, Information Assurance.		
1. TYPED OR PRINTED NAME	2. RANK/CIVILIAN GRADE	3. PHONE NUMBER
4. SIGNATURE	5. DATE	

SECTION IX - STANDARD CONTRACT LANGUAGE

1. General security requirements and guidance: The security requirements described below apply to all contract personnel (including employees of the prime Contractor ("Contractor") and all subcontractor employees) supporting the performance requirements of this contract. The Contractor is responsible for compliance with these security requirements. Questions regarding security matters shall be addressed to the designated Government representative (e.g., Contracting Officer Representative (COR), Requiring Activity (RA) representative, or Contracting Officer (if a COR or other RA representative is not appointed)). Contract personnel are critical to the overall security and safety of US Army Corps of Engineers (USACE) installations, facilities and activities, and security awareness training contributes to those efforts. The Department of Defense (DoD) and Army security training requirements specified below, if applicable, are performance requirements; all applicable contract personnel shall complete initial training within 30 days of contract award or the date new contract personnel begin performance on the contract. Within five business days from the completion of training, the Contractor shall provide written documentation (e.g., email or memorandum) to the Government representative. The documentation shall include the names of contract personnel trained and which training they completed; the Contractor shall maintain training records as part of their contract files and be prepared to provide copies of training certificates to the Government representative. Contractor personnel and vehicles are subject to search when entering federal installations. Additionally, all contract personnel shall comply with Force Protection Condition (FPCON) measures, Random Antiterrorism Measures (commonly referred to as "RAMs"), and Health Protection Condition (HPCON) measures. The Contractor is responsible for meeting performance requirements during elevated FPCON and/or HPCON levels in accordance with applicable RA plans and procedures --this includes identifying mission essential and non-mission essential personnel. In addition to the changes otherwise authorized by the changes clause of this contract, should the FPCON or HPCON levels at any individual facility or installation change, the Government may implement security changes that affect contract personnel. The Contractor shall ensure all contract personnel are aware of their security responsibilities, including any site-specific requirements identified in local policies or procedures.

2. Antiterrorism (AT) Level I training: All contract personnel requiring routine access to Army installations, facilities, and controlled access areas, or requiring network access shall complete initial and annual refresher AT Level I awareness training. Online AT Level I awareness training is available at https://jko.jten.mil/ (website subject to change).

3. Physical security and access control requirements: All contract personnel requiring physical access to a federal installation or facility shall comply with the access control procedures of that location. Contract personnel requiring unescorted access to meet contract performance requirements on a DoD installation in the US shall be vetted by the installation/facility Provost Marshal/Directorate of Emergency Services/Security Office using the National Crime Information Center-Interstate Identification Index (commonly referred to as "NCIC-III") and Terrorist Screening Database (commonly referred to as "TSDB"). Contract personnel shall comply with all personal identity verification requirements specified in installation/facility policies and procedures. Contract personnel who do not meet requirements for unescorted access to USACE facilities shall coordinate escorted access with the Government representative, as needed. Contract personnel who receive keys, access cards, or lock combinations that provide access to government-owned property shall comply with key and lock control procedures of the RA.

4. Contract personnel requiring a common access card (CAC): Contract personnel will be issued a common access card (CAC) only if duties involve one of the following: (1) both physical access to a DoD facility and access to DoD information systems or networks; (2) remote access to a DoD information system or network using DoD-approved remote access procedures; or (3) physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of 6 months or more. Before CAC issuance, contract personnel must have, at a minimum, a favorably adjudicated Tier 1 investigation or an equivalent or higher investigation in accordance with applicable Army regulations and Homeland Security Presidential Directive-12 (HSPD-12). At the discretion of the RA, an initial CAC may be issued based on a favorable review of a fingerprint check and a successfully scheduled Tier 1 investigation with the National Background Investigations Bureau. The RA provides contract personnel with additional information and forms to initiate the CAC issuance process, and/or to initiate background investigations, when required. Contract personnel shall complete these processes within established timelines to avoid delays.

5. Security requirements for contract performance outside the US: For contract performance requirements that involve services or delivery in a foreign country, the Contractor shall comply with the requirements of DFARS clause 252.225-7043. For performance requirements that involve contract personnel accompanying or supporting US Armed Forces deployed outside the US, the Contractor shall comply with the requirements of DFARS clause 252.225-7040. Contract personnel accessing DoD or other federal facilities outside the US shall comply with applicable Status of Forces Agreements and Geographic Combatant Command requirements. Prior to contract personnel traveling outside the US, the Contractor shall provide documentation of AT, OPSEC, and other required training to the Government representative. Additionally, contract personnel shall comply with requirements specified in the DoD Foreign Clearance Guide, including country and theater clearance processes.

6. Suspicious Activity Reporting training (e.g. iWATCH, CorpsWatch, or See Something, Say Something): All contract personnel shall receive initial and annual refresher training from the RA representative on the local suspicious activity reporting program. This locally developed training provides contract personnel with general information on suspicious behavior, and guidance on reporting suspicious activity to the project manager, security representative or law enforcement entity.

7. Contract personnel requiring access to Government information systems: All contract personnel with access to a government information system (including USACE business systems and CAC-enabled websites) shall comply with applicable DoD and Army regulations, and shall use the organization's UserID-Password Administration and Security System (U-PASS) at commencement of services to request network user accounts. Contract personnel shall complete DoD Information Assurance Awareness training prior to accessing information systems, and annually thereafter.

8. Contracts requiring a formal OPSEC program: The Contractor shall develop an OPSEC SOP/Plan within 90 days of contract award. The OPSEC SOP/Plan shall be reviewed and accepted by the RA OPSEC Officer. This plan will include a process to identify critical information, where it is located, who is responsible for it, how to protect it, and why it needs to be protected. In accordance with Army and DoD regulations, the contractor shall have a certified Level II OPSEC coordinator, who shall ensure OPSEC compliance during contract performance.

9. Training requirements for the protection of sensitive information: All contract personnel with access to critical information (as identified in the RA's OPSEC Program) shall complete initial and annual refresher OPSEC Level I Awareness training, which is available at the following websites: https://www.iad.gov/ioss/, or http://www.cdse.edu/catalog/operations-security.html (websites subject to change). All contract personnel with access to Controlled Unclassified Information (CUI) shall complete initial and annual refresher CUI training in accordance with applicable Army policy.

10. Information Assurance (IA)/Information Technology (IT) requirements: All contract personnel performing IA/IT services must comply with DoD training and certification requirements specified in DoD 8570.01-M, Information Assurance Workforce Improvement Program, and maintain required background investigations specified in RA policy. Contract personnel shall provide the Government representative with documentation of certification(s) prior to performing on the contract. In accordance with applicable DoD, Army, and USACE regulations, the Contractor shall ensure that all information systems (IS) and platform information technology (PIT) systems developed and/or supported under this contract comply with cybersecurity and architectural requirements, including, but not limited to: security technical implementation guides (STIG)(e.g., the current version of the Application Security and Development STIG, and the internet access point (IAP) demilitarized zone (DMZ) STIG), and the use of security controls developed under the risk management framework documentation for the system or platform. The Contractor shall address questions regarding these provisions to the Government representative, who will coordinate between the Contractor and the USACE Chief Information Officer (CIO).

11. Contracts requiring handling or access to classified information: The prime Contractor shall have a Facility Clearance (FCL) at the appropriate level prior to performance on the contract; the RA will sponsor the prime contract company in obtaining the FCL. All cleared contract personnel shall comply with the FCL requirements, as well as applicable laws and regulations regarding contractor access to national security information. For classified contracts, the RA will generate the DD Form 254, which will be attached to the contract.

12. Threat Awareness Reporting Program: All contract personnel who maintain an active security clearance shall receive initial and annual refresher training on the Threat Awareness and Reporting Program (commonly referred to as “TARP”), provided by a Counterintelligence Agent. As determined by the servicing Counterintelligence Agent for the RA, contract personnel may complete web-based TARP training.

13. Escorting in classified and/or sensitive areas: In accordance with applicable regulations, all contract personnel who do not possess the appropriate security clearance or access privileges will be escorted in areas where they may be exposed to classified information or operations, sensitive information or activities, or restricted areas.

14. Pre-screen candidates using E-Verify Program: Contractors shall comply with the requirements set forth in FAR clause 52.222-54 Employment Eligibility Verification and FAR Subpart 22.18 in using the E-Verify Program at (https://www.e-verify.gov/) (website subject to change) to meet the contract employment eligibility requirements. Contractors are encouraged to cooperate with Federal and State agencies responsible for enforcing labor requirements to include eligibility for employment under United States immigration laws in accordance with FAR 22.102-1(i). An initial list of verified/ eligible candidates shall be provided to the COR no later than three business days after the initial contract award. When contracts are with individuals, the individuals will be required to complete a Form I-9, Employment Eligibility Verification, and submit it to the Contracting Officer to become part of the official contract file.

15. Contracts requiring armed security guards: All contract personnel performing contract security guard duties shall comply with the Individual Reliability Program in accordance with AR 190-56 (The Army Civilian Police and Security Guard Program), as well as applicable installation, facility and area commander installation/facility policies and procedures regarding storing weapons and ammunition in accordance with AR 190-11 (Physical Security of Arms Ammunition, and Explosives).

16. Contracts requiring delivery of food and water: The supplies delivered under this contract shall be transported in delivery conveyances maintained to prevent tampering with and/or adulteration or contamination of the supplies, and if applicable, equipped to maintain a prescribed temperature. All delivery vehicles and storage locations are subject to inspection at any time by the COR, Post Veterinarian, law enforcement officers, or other RA representatives authorized to conduct such inspections. When the sanitary conditions of the delivery conveyance have led, or may lead to product contamination, adulteration, constitute a health hazard, the delivery conveyance is not equipped to maintain prescribed temperatures, or the transport results in product “unfit for intended purpose,” supplies tendered for acceptance may be rejected without further inspection. As the holder of a contract with the DoD, the Contractor shall ensure that all products and/or packaging have not been tampered with or contaminated. The Contractor shall ensure all delivery conveyances are always locked or sealed, except when actively loading or unloading. Unsecured vehicles shall not be left unattended. All incoming truck drivers shall provide adequate identification upon request. In the event of an identified threat to a delivery location, or a heightened force protection/Homeland Security threat level, the Contractor may be required to adjust delivery routes to minimize vulnerability risks and enable direct delivery to DoD facilities.