U.S. Army Corps of Engineers (USACE)

CONTRACT REQUIREMENTS PACKAGE SECURITY REVIEW COVER SHEET (Non-Army Customer)

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

SECTION I - REQUIREMENT INFORMATION

1. CONTRACT or REQUIREMENTS TITLE	2. LOCATION
3. SUPPORTING USACE ORGANIZATION	4. SUPPORTED SERVICE/AGENCY

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), etc.) for a USACE contract awarded on behalf of an agency or organization outside the Department of the Army (e.g., USAF, DHHS, FEMA). These non-Army customers of USACE are the Requiring Activity (RA) for the applicable contract action. Army policy requires a coversheet to be included in all contract requirements packages, except for supply contracts under the simplified acquisition level threshold, field ordering officer actions, and government purchase card purchases. This form meets the coversheet standard, while not imposing Army-specific security requirements on non-Army customers. Use of this form does not preclude the RA or the applicable USACE Contracting Office from incorporating additional security-related language into contracts. In accordance with HQ-USACE policy, the RA must complete the coversheet prior to submitting requirements packages to the supporting contracting activity. The RA representative completing this form shall be familiar with contracting processes and policies (e.g., Federal Acquisition Regulation (FAR), and any other regulations applicable to the RA's agency) and their Agency's security policies and requirements. The USACE representative reviewing and signing this form may perform any supporting role for the contract (e.g., Project or Program Managers, Quality Assurance Specialists, or similar duties).

SECTION III - STANDARD CONTRACT LANGUAGE

The RA Representative shall consider the applicability of each requirement, and check each block as "Yes" or "N/A." If the standard PWS/SOW language text found in Section VIII 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. If the standard PWS/SOW language applies but additional language is required, check "Yes" and include both the standard language and additional contract specific language in the PWS/SOW. If standard PWS/SOW language does not apply, check "N/A."

SECTION IV - REQUIRED CLAUSES

Required Clause(s) (*see Section VIII for sample language*)	YES	N/A
Agency or Service-Specific Requirements (See Section V).	☐	☐
1a. General security requirements and guidance (DoD Components Only).	☐	☐
1b. General security requirements and guidance (Other Federal Agencies).	☐	☐
2. Physical security and access control requirements (DoD Components Only).	☐	☐
3. Contractor personnel requiring a common access card (CAC) (DoD Components Only).	☐	☐
4. Contractor personnel requiring a personal identity verification (PIV) credential (Other Federal Agencies).	☐	☐
5. AT Level I training (DoD Components Only).	☐	☐
6. Training requirements for the protection of sensitive information.	☐	☐
7. Counterintelligence Awareness Training (DoD Components Only).	☐	☐
8. Contracts requiring a formal OPSEC program (DoD Components Only).	☐	☐
9. Contract personnel requiring access to Government information systems.	☐	☐
10. Contracts requiring handling or access to classified information.	☐	☐
11. Escorting in classified and/or sensitive areas.	☐	☐
12. Pre-screen candidates using E-Verify Program.	☐	☐
13. Contracts requiring delivery of food and water.	☐	☐

SECTION V - REMARKS	
1. CONTRACT TITLE	2. LOCATION
(The RA may add general information below or use this space to include additional agency or service-specific requirements.)	

SECTION VI - REQUIRING ACTIVITY POINT OF CONTACT SIGNATURE		
I have reviewed the performance requirements and annotated applicable clauses in accordance with governing laws, policies, or regulations.		
1. TYPED OR PRINTED NAME	2. RANK/CIVILIAN GRADE	3. PHONE NUMBER
4. SIGNATURE	5. DATE	

SECTION VII - USACE POINT OF CONTACT SIGNATURE		
I have coordinated with the RA to ensure applicable clauses from this coversheet are included in the requirements document.		
1. TYPED OR PRINTED NAME	2. RANK/CIVILIAN GRADE	3. PHONE NUMBER
4. SIGNATURE	5. DATE	

SECTION VIII - STANDARD CONTRACT LANGUAGE

1a. General security requirements and guidance (DoD Components Only): 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)). The Department of Defense (DoD) and Service-specific security requirements specified below, if applicable, are performance requirements. All contract personnel shall complete applicable initial training within 30 days of contract award, or the date new contract personnel begin performance on the contract. The Contractor shall maintain security training records in accordance with applicable RA policies. 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 security 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.

1b. General security requirements and guidance (Other Federal Agencies): 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 all security requirements and any others promulgated by the Requiring Activity (RA). Questions regarding security matters shall be addressed to the designated Government representative (e.g., Contracting Officer Representative (COR), RA representative, or Contracting Officer (if a COR or other RA representative is not appointed)). In circumstances where access to a DoD installation or facility is necessary to meet contract performance requirements, contractor personnel shall comply with that agency's security requirements (e.g., access control procedures, etc.). Contractor personnel entering federal buildings and non-DoD installations shall follow applicable access control procedures and are subject to search in accordance with Interagency Security Committee (ISC) regulations.

2. Physical security and access control requirements (DoD Components Only): All contract personnel requiring physical access to a DoD installation or facility shall comply with the access control procedures of that location. Contract personnel requiring unescorted access on a DoD installation in the US to meet contract performance requirements 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 DoD-owned 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. Reference: DoDM 5200.08, Volume 3, "Physical Security Program: Access to DoD Installations."

3. Contract personnel requiring a common access card (CAC) (DoD Components Only): 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 DoD regulations. 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.

4. Contract personnel requiring a personal identity verification (PIV) credential (Other Federal Agencies): Contract personnel will only be issued a personal identity verification (PIV) credential when necessary to meet contract performance requirements, and in accordance with Homeland Security Presidential Directive-12 (HSPD-12) and RA policy.

5. Antiterrorism (AT) Level I training (DoD Components Only): All contract personnel requiring routine access to DoD installations, facilities, and controlled access areas, or requiring network access shall complete initial and annual refresher AT Level I awareness training for the first three years of performance on a DoD contract, and triennially thereafter. The RA may also provide additional awareness material to contract personnel regarding suspicious activity reporting. Online AT Level I awareness training is available at https://jkodirect.jten.mil/ (website subject to change). Reference: DoDI O-2000.16, Volume 1, "DoD Antiterrorism Program Implementation: DoD Antiterrorism Standards."

6. Training requirements for the protection of sensitive information (DoD Components Only): All contract personnel with access to critical information (as identified in the RA's Operations Security (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). Reference (DoD Only): DoDM 5205.02, "DoD Operations Security (OPSEC) Program Manual." All contract personnel with access to Controlled Unclassified Information shall complete training in accordance with applicable DoD or other federal agency policy. Reference (DoD Only): DoDD 5200.48, "Controlled Unclassified Information (CUI)."

7. Counterintelligence Awareness Training (DoD Components Only): All contract personnel who maintain an active security clearance shall receive initial and annual refresher training on counterintelligence awareness, consistent with applicable training guidance for the RA. Reference: DoDD 5240.06, Counterintelligence Awareness and Reporting (CIAR).

8. Contracts requiring a formal OPSEC program (DoD Components Only): 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 DoD and Service regulations, the contractor shall have a certified Level II OPSEC coordinator responsible for OPSEC compliance during contract performance. Reference: DoDM 5205.02, “DoD Operations Security (OPSEC) Program Manual.”

9. Contract personnel requiring access to Government information systems: Contractor personnel shall be granted access to DoD or other Federal agency government information systems only when required to meet contract performance requirements. For DoD contracts, contract personnel shall complete DoD Information Assurance Awareness training prior to accessing information systems, and annually thereafter. For other federal agency contracts, contract personnel shall comply with applicable agency policies.

10. Contracts requiring handling or access to classified information: The Contractor shall comply with DoD or other federal agency industrial security policies and procedures. The 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 included with the solicitation and contract. References: 32 C.F.R. § 117 and DoDM 5220.22, “National Industrial Security Program Operating Manual (NISPOM).”

11. Escorting in classified and/or sensitive areas: In accordance with RA policies and procedures, 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 other restricted areas.

12. 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 RA's COR or similar point of contact 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.

13. 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. 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 alternative locations.