Performance Work Statement (PWS)

Defense Activity for Non-Traditional Education Support (DANTES)
Online College and Career Planning Counseling Tool
May 28, 2026

1.0 INTRODUCTION

The Defense Activity for Non-Traditional Education Support (DANTES) executes a portfolio of Defense education programs that help Service members achieve their personal and professional education goals. DANTES, a component of the Defense Human Resources Activity (DHRA), accomplishes this by developing and implementing off-duty, Voluntary Education (VolEd) programs and supporting activities related to Department of Defense's (DoD) education functions. DANTES leverages economies of scale to provide military Service branches with education programs which promote:

- Quality education opportunities
- College readiness and student success
- VolEd community support

2.0 BACKGROUND

The Department of Defense Instruction (DODI) 1322.25 paragraph 6.c, requires DANTES to consolidate management of education programs to prevent duplication of effort among the services. Personnel in each of the Services require customized college and career counseling services which include interest assessments related to both college and career choices. As such, DANTES manages the delivery of an enterprise-wide solution for a personalized college and career planning counseling service. The most cost effective and efficient method of delivering a college and career planning tool for a large, widely dispersed audience is to provide access to a commercially available web-based resource. The online program requires continuous availability for personnel serving at locations around the world. The core functional requirements for the online college and career planning counseling tool were established in coordination with the DOD Inter-Service Voluntary Education Board (IVEB), and the Chief of DOD Voluntary Education.

3.0 SCOPE

The Contractor shall provide the personnel, management and materials necessary for access to an online resource that shall allow military members self-paced counseling assistance resulting in a career and education pathway customized for each individual user. This resource shall help military members plan for an appropriate career based on personal information by assessing interests, skills, and work values. The tool shall provide career options aligned to a user's self-assessment, an education pathway for specific career options, prepare users for a job search; and facilitate the job search process. The tool shall be based on sound career theory and up-to-date information and resources of state and national colleges, scholarship, labor, and occupational information integrated seamlessly to the respective databases. This college and career planning counseling program will assist Service members in identifying education and career pathways in

preparation for their eventual transition to the civilian workforce. The tool shall be available online, 24/7, 365 days per year and shall be available for unrestricted usage for all active, reserve, and National Guard military members (Air Force, Army, Navy, Marine Corps, Space Force, and Coast Guard). Service members who access the tool and establish an account during the subscription period shall have ~~lifetime~~ unlimited access to their portfolio, individual assessments and documents.

4.0 REQUIREMENTS *The Contractor shall*:

The contractor shall provide access to a commercially available online college and career planning tool. The tool shall be provided as a service on a subscription basis in accordance with this PWS and shall not become the property of the Government. The contractor is responsible for designing and developing all content for the college and career counseling resource. The following functionality, miscellaneous support, system availability & technical support, and reporting requirements apply:

4.1 Availability and Functionality - Online College and Career Planning Counseling Tool

The college and career planning counseling tool provided as a service herein shall have the following functionality:

4.1.1 Web-based access available to an unlimited number of military personnel under a dedicated URL.

4.1.2 User registration, account set-up and login shall be established for individual users. Online registration shall capture branch of military service and military installation location. Separate registration shall be provided for military counselors/administrators who will require access to increase program familiarity. Users shall be able to directly reset passwords or retrieve their user names.

4.1.3 Tutorials, videos, and text-based information shall be provided for users and administrators as necessary to assist in navigating the online tool and enhance the user experience.

4.1.4 Use of the tool shall be self-paced and available on an unrestricted basis.

4.1.5 Users shall be allowed to exit and re-enter the site as often as necessary at no additional cost to the Government. Start and stop options shall be available for saving assessments and career management information.

4.1.6 A detailed self-interest assessment shall be administered to determine a user's career interests, work values, and work skills.

4.1.7 A personal career plan which aligns potential occupations and education requirements with the interest assessment shall be provided.

4.1.8 Customized career and education pathways based on assessment information shall be provided along with a customized menu of resources.

4.1.9 User options shall be available to explore related career, occupational, and educational information.

4.1.10 Guidance for planning military personnel transition to the civilian workforce and future employment to include: resume writing guidance, interview question samples, use of social networking sites, and conducting internet job searches.

4.1.11 Search capability for civilian occupations by Military Occupation Specialty (MOS).

4.1.12 Capability to enter Armed Services Vocational Aptitude Battery (ASVAB) scores and receive a list of civilian occupations aligned to scores. Users shall be able to filter this list by educational entry level, industry cluster, degree of expected job growth, and/or median annual salary for the state in which they expect to work.

4.1.13 Online search capability for education and financial aid information, specific career and education information for military service members and a link to: http://www.benefits.va.gov/gibill.

4.1.14 Links to academic financial aid support information, U.S. Department of Education accredited post-secondary schools, and U.S. Department of Labor career outlook information.

4.1.15 Information related to education benefits for Service members and Veterans on the Department of Veterans Affairs – GI Bill of Rights. Information shall include links to military transition centers and military–specific transitional job services sites.

4.1.16 Links to military-friendly employers.

4.1.17 Job search tool offering a variety of search methods to include state job banks, Google search by occupation, and links to current employment websites~~ such as Monster and CareerBuilder~~.

4.1.18 Instructions on how to find job openings and how to use career fairs. Additional search criteria:

- Identify nearby one-stop centers.
- Identify military-friendly employers.
- Find civilian jobs by translating Military Occupation Specialty (MOS) to civilian occupations.

4.1.19 A secure electronic portfolio shall be created for each user that serves as a repository for all self-interest assessments, career plans, career and education pathways, and other applicable career information. Items stored in the portfolio include assessment scores; descriptions of favored occupations, programs of study, postsecondary institutions, and sources of financial aid; resumes, cover letters, and reference lists; and uploaded items such as short videos, work samples, earned certificates, and transcripts. Once an eligible

user has an established account, the user shall have ~~lifetime~~ unlimited access to their electronic portfolio. The user shall be able to access their electronic portfolio at any time. Documents stored in the portfolio exclusively belong to the uploading user and are excluded from the data rights described in Section 7.10. Should the online tool need to be decommissioned for any reason, notice must be provided to all registered users by email a minimum of 30 calendar days prior to the tool going offline.

4.2 Contractor Provided Miscellaneous Support

4.2.1 The contractor shall provide promotional and marketing materials on the college and career planning counseling tool in online digital format and, if necessary, print format. The contractor shall determine the design, message, and quantities for all marketing materials. The contractor is responsible for sending print materials directly to requesting education services offices if required.

4.2.2 The contractor shall provide Webinar training not to exceed more than 1 event per month. The Webinar content shall promote the usage of the online college and career planning tool, provide training on the use of the tool, and highlight tool features to military education professionals, counselors, and service members.

4.3 System Availability and Technical Support

4.3.1 The contractor shall provide all maintenance, sustainment, systems hardware, and hosting necessary to meet system availability requirements.

4.3.2 The system must have a minimum availability of 98 percent measured monthly.

4.3.3 The contractor shall provide technical support for students and administrators via telephone or email. Technical support inquiries shall be responded to within 24 hours of receipt during the business hours of Monday – Friday, 7:00 a.m. - 6:00 p.m. (Central Time). Additionally, information shall be available on the website to assist users with technical troubleshooting.

4.3.4 The contractor shall have the ability to add notifications to home page or login page of program (i.e. notification if system is down, scheduled maintenance, content changes, etc.)

4.4 Reporting

4.4.1 Quarterly Reports: The contractor shall provide quarterly usage reports to include the following information:

4.4.1.1 Registrations - New enrollees for the program.

4.4.1.2 Interest Assessments usage:

4.4.1.2.1 Assessments Completed - Number of Pre-Assessments completed ~~in~~ addressing each of the constructs ~~assessments~~ (career interests, work values and work skills) and identified completion by parameter of service branch. This will include monthly usage and an overall cumulative total for all service branches.

4.4.1.2.2 Counselor/Administrator Training request - Number of military counselors/administrators requesting access.

4.5 Section 508 Requirements

The Contractor shall comply with Section 508 of the Rehabilitation Act of 1973 (29 U.S.C 794) and the Architectural and Transportation Barriers Compliance Board's (U.S. Access Board) information and communication technology (ICT) accessibility standards at 36 CFR 1194.1 for requirement deliverables. The applicable standards are available at https://www.access-board.gov/ict/. The following standards have been determined to be applicable to this contract:

Technical Standards
E205 – Electronic Content
E208 – Support Documentation and Services

5.0 DELIVERABLES

5.1 Format for Deliverables - Contractor format for written deliverables is acceptable. All written deliverables shall be provided as a Defense Manpower Data Center (DMDC) compliant Microsoft electronic document or other electronic format as appropriate. All imbedded documents shall be Microsoft Office Suite compatible and DMDC compliant, unless otherwise agreed upon.

5.2 Review of Deliverables - Deliverables provided under this contract shall be submitted to the Government Contracting Officer Representative (COR). The COR will have ten working days after receipt to review deliverables, and provide comments, corrections, and recommended changes to the contractor. The contractor shall incorporate agreed upon changes and submit revised deliverables to the COR within 10 working days after receipt or unless otherwise agreed upon by the parties.

5.3 Schedule of Deliverables

All deliverables will be reviewed for timeliness, accuracy and format. If a deliverable due date falls on a weekend or holiday, the Contractor shall submit the deliverable on the last work day prior to the due date. In fulfillment of this effort, the Contractor shall provide the following deliverables to the COR.

Deliverable	PWS Ref	Due Date	Delivered To
Online College and Career Planning Tool	4.1	~~Beginning of Contract Award~~Within 30 calendar days after	Service members

		contract award	
Quarterly Usage Data	4.4	Within 7 days of each quarter beginning 3 months after contract award	COR

Marketing and Promotional Material	4.2.1	TBD by Contractor and COR	COR
Webinars	4.2.2	NTE one per month	Assessment users

5.4 The contractor shall report contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via the System for Award Management (SAM) (https://sam.gov) in accordance with DFARS 252.204-7023.

6.0 CONTRACTOR TRAVEL

Travel is not anticipated for this requirement. Should travel become necessary, a proposal will be requested and the contract modified to reflect travel.

7.0 RECORDS MANAGEMENT

7.1 Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

7.2 In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

7.3 In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

7.4 Defense Human Resources Activity and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of Defense Human Resources Activity or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Contracting Officer's Representative (COR). Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to the COR and the Defense Human Resources Activity Component Records Management Officer at dodhra.mc-alex.dhra-hq.mbx.records@mail.mil so DHRA may report promptly to NARA in accordance with 36 CFR 1230.

7.5 The Contractor shall immediately notify the COR upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know in accordance with all applicable privacy, security, and information protection policies. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or

maintained on the Government's behalf, without the express written permission of the COR. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to DHRA control or the Contractor must hold it until otherwise directed.

Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the COR. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (7.4).

7.6 The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and Defense Human Resources Activity guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

7.7 The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with Defense Human Resources Activity policy.

7.8 The Contractor shall not create or maintain any records containing any non-public Defense Human Resources Activity information that are not specifically tied to or authorized by the contract.

7.9 The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

7.10 The Defense Human Resources Activity owns the rights to all data and records produced as part of this contract. The contractor shall not include any contractor markings on deliverables created under the contract. All deliverables under the contract are the property of the U.S. Government for which Defense Human Resources Activity shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. The contractor shall not use or disclose any data or deliverables under this contract for any purposes other than performing the contract, unless expressly approved by the Government.

8.0 SECURITY

8.1 Personnel Security. Overarching security requirements are UNCLASSIFIED. Contractor and Subcontractor personnel working on behalf of the federal government to compile information pertaining to Service members, including active, reserve, and National Guard

personnel from the Air Force, Army, Navy, Marine Corps, Space Force, and Coast Guard, must safeguard their information as Controlled Unclassified Information (CUI). Contractor personnel in roles that administer the web-based tool capable of unlimited registration and management of individual accounts must comply with federal cybersecurity and personnel security regulations.

8.1.1 Position Designation. The Contractor and Subcontractor personnel on this contract will be designated performing in noncritical-sensitive (moderate risk) or non-sensitive (low risk) positions with unclassified access.

8.1.2 Tier 3 (T3) Investigation. Individuals with access to, or the ability to, aggregate and extract large-scale data (more than 100,000 records) containing Personally Identifiable Information (PII) from an automated records repository must obtain and maintain a Tier 3 (T3) background investigation (BI) and adjudication or determination.

8.1.3 Tier 1 (T1) Investigation. At a minimum, personnel whose access to Service members' PII is limited to data entry or single-search functions require a favorably adjudicated Tier 1 (T1) BI.

8.1.4 Personnel designations align with investigative requirements outlined by Defense Counterintelligence and Security Agency (DCSA) and is in accordance with the DoD Personnel Security Program, as defined in DoDI 5200.02, DoDM 5200.02. Specifically, Title 32, Code of Federal Regulations Part 156 applies to unclassified contracts, and Part 117 applies to contracts covered by the National Industrial Security Program (NISP).

8.1.5 No employee may perform under this contract or have access to DoD information or systems under this contract until they have completed the Tier investigation that meets the requirement or be in the process of a Personnel Security Investigation (PSI) with a minimum of interim eligibility approval.

8.2 Staffing. The personnel supporting this contract who require access to access to Service members' information or CUI, such as PII, must be Citizens of the United States. The citizenship requirement also applies to personnel assigned or working on the contract at any remote sites.

8.3 Onboarding. All Contractor personnel working on behalf of DHRA contracts, regardless of their access level, must be processed using the DHRA onboarding system (EAFi or DoD Service Center). They must also provide a completed Defense Logistics Agency Headquarters (DLAH) Form 1728, Request for HQC Contractor Badge and/or Information Technology (IT) Access, using a secure method (e.g., encrypted email or DoD SAFE). The DHRA Security and DLA Personnel Security (PERSEC) offices will then validate that the contractor meets DoD background investigation requirements.

8.4 Listing of employees & Clearance Documentation. The Contractor shall maintain a current listing of employees. Within 10 calendar days of contract award, the Contractor shall provide the COR with a list of all personnel assigned to the contract or task order. The

personnel list must include the following information: contract number, contract expiration date, employee information (full legal names), DHRA center/office, location of performance, clearance level needed (e.g., Top Secret, Secret, Confidential or None [for unclassified access]), and IT access needed (e.g., privilege, authorize or other). The Contractor shall provide the COR and DHRA Security with an updated list whenever personnel status or information changes.

8.5 Access to Sensitive Information. To the extent that the work under this contract requires the Contractor to have access to DoD sensitive information, the Contractor shall, upon receipt, treat such information as sensitive and safeguard it from unauthorized use and disclosure. The Contractor shall not appropriate such information for its own use or disclose such information to third parties unless specifically authorized by the Government in writing.

8.5.1 The Contractor shall only allow access to sensitive information to those employees who need it to perform services under this contract and who have acknowledged that it shall be used solely for that purpose. The Contractor shall prevent its employees from discussing, divulging, or disclosing any sensitive information to any person or entity except those within the Contractor's organization directly performing the contract.

8.6 Operations Security (OPSEC) Requirements. The Contractor is not required to develop an OPSEC Plan. However, the Contractor shall comply with DoD Directive 5205.02E and the requiring activity's OPSEC program. Contractor employees must complete Level I OPSEC Awareness training. New employees must be trained within 30 calendar days of their reporting for duty and annually thereafter. The Contractor shall maintain all OPSEC training records and shall provide copies to the COR upon request.

8.7 Personal Identifiable Information (PII) and Tier Investigations. All personnel supporting this contract must protect PII data according to the Privacy Act of 1974. Personnel requiring access to Information Technology (IT) or access to DoD Information Systems that contain military active duty, guard, or reservists' PII or information pertaining to Service members that are otherwise protected from disclosure, where such access has the potential to cause serious damage to national security, must be vetted accordingly and protect the data. Background Investigations (BI) levels required for each job function or necessary access include, but are not limited to, the following:

8.7.1 Tier 5/Tier 5R for Special-Sensitive/Critical-Sensitive – High Risk: All personnel with administrative capabilities in a system storing PII, personnel security investigations, or adjudication determinations require a Tier 5 (T5) BI.

8.7.2 Tier 3/Tier 3R for Noncritical-Sensitive – Moderate Risk: All personnel with the ability to aggregate or extract military PII en masses from an automated records repository require, at a minimum, a favorably adjudicated Tier 3 (T3) BI or equivalent.

8.7.3 Tier 1 for Non-Sensitive – Low Risk: All Personnel whose access to military PII is limited to data entry or singular search capability require, at a minimum, a favorably adjudicated Tier 1 (T1) BI.

8.7.4 The Contractor shall report any privacy breach immediately to the DHRA Privacy Office and secondly to the COR.

8.8 Controlled Unclassified Information Requirements for DoD Contractors. The following procedures will be used to protect Controlled Unclassified Information (CUI) documents and materials:

8.8.1 HANDLING: Access to CUI material shall be limited to those employees needing the material to perform their duties. The CUI marking is assigned to documents and material created by a DoD User Agency. CUI is not a classification, but requires extra precautions to ensure it is properly safeguarded and disseminated and is not released to the public without government authorization.

8.8.2 MARKING: The Contractor shall mark unclassified documents containing CUI as follows: “CUI" at the top and bottom of each page, include the CUI warning box, and the CUI Designation Indicator Block as required in DoDI 5200.48.

8.8.2.1 Mark other records such as computer print outs, photographs, films, tapes, or slides in accordance with DoDI 5200.48 so the receiver or viewer knows that it contains CUI material.

8.8.2.2 Mark a message containing material in accordance with DoDI 5200.48. Unclassified messages containing CUI material must show the abbreviation (CUI) before the text begins.

8.8.2.3 Ensure documents transmitting CUI material call attention to any attachments containing CUI.

8.8.2.4 CUI material released to a contractor by a DoD user agency must have the following statement on the front page or cover:

THIS DOCUMENT CONTAINS CUI MATERIAL AND MUST BE REVIEWED BY A GOVERNMENT REPRESENTATIVE UNDER THE REQUIREMENTS OF DODI 5200.48, DODI 5230.09, and DODI 5230.29.

8.8.3 STORAGE: The Contractor shall, place CUI material in an out-of-sight location during normal work hours, if the work area is accessible to persons who do not have an authorized government purpose for access to the material. After normal duty hours, the Contractor shall store CUI material to prevent unauthorized access by filing it with other unclassified records in unlocked files or desks when internal building security is provided and the file is marked as CUI. When there is no internal security, locked buildings or

rooms usually provide adequate after hours protection. For additional protection, store CUI material in locked containers such as file cabinets, desks, or bookcases.

8.8.4 TRANSMISSION: CUI documents and materials may be transmitted via first class mail, parcel post or, for bulky shipments, fourth class mail. Within the CONUS discussion of CUI material on the telephone is authorized if necessary for the performance of the contract and no alternative is available. Electronic transmission of CUI (voice, data, or facsimile) should be by using approved and secure communications systems whenever practical. If there is a fax transmission, the sender must ensure the intended receiver is available to receive it or a cover sheet will be used to allow carrying it to the final recipient to avoid unauthorized disclosure of the CUI.

8.8.5 RELEASE: CUI material shall not be released outside of the contractor's facility except to the representative of DoD or DHRA.

8.8.6 DESTRUCTION: When the CUI material no longer meets the threshold for safeguarding and dissemination, the Contractor shall immediately decontrol it, process it through the records management process, and destroyed by the approved methods identified in DoDI 5200.48 to preclude its disclosure to unauthorized individuals by rendering it unreadable, indecipherable, and irrecoverable.

8.9 Position of Trust (POT) Requirements. The Contractor shall provide the COR with a list of personnel requiring unclassified access no later than five business days after contract award and within three business days of any change.

8.9.1 Reciprocity Consideration. In accordance with DoD standards outlined in Executive Order E.O 13488, existing Personnel Security Investigations (PSIs) for contractor personnel will be validated or assessed for reciprocity. Contractor personnel shall provide additional information if requested by the DHRA and DLA Security office for DCSA re-adjudication or eligibility assessments. PSI equivalency will be determined according to the investigative alignments provided by DCSA. Reciprocity considerations include verifying any break in federal service (e.g., U.S. Military, U.S. Civilian or U.S. Contractor) exceeding 24 months since the last favorable investigation.

8.9.2 Government Responsibilities. The Government is responsible for funding Contractor personnel PSIs or sponsoring a DoD-determined equivalent background check when eligibility is required for Position of Trust without access to classified information. The Contractor shall ensure the COR and Government Security Office are informed of Contractor personnel requiring sponsored PSIs.

8.9.3 Tier Application Requirements. DCSA offers three-tier Personnel Security Investigations (PSI): Tier 5 (High Tier), Tier 3 (Moderate Tier) and Tier 1 (Low Tier). Contractor personnel requiring a Tier PSI shall provide an FBI fingerprint check, proof of U.S. Citizenship, and a Personnel Security Questionnaire (PSQ). The Standard Form (SF) SF86 must be used for High or Moderate Tiers, and SF85 for Low Tier, using the National Background Investigation Services (NBIS) electronic Application (eApp).

Contractor personnel shall provide all requested information pursuant to the Privacy Act of 1974 when requested by the Government. The Government Security Office will provide instructions, specific to the individual case and designated Tier, on how to access the NBIS system. For information, visit NBIS website at https://www.dcsa.mil/is/nbis/

8.9.4 Interim Determinations. DLA Security will assess each Tier PSI application package, including FBI fingerprint check results, Proof of U.S. Citizenship, and PSQ for interim eligibility. The Contractor shall not assign personnel to duties supporting the Government contract before interim approval is granted. To maintain interim Position of Trust eligibility, personnel must:

8.9.4.1 Comply with all personnel security requirements specified by DHRA and DLA Security;

8.9.4.2 Obtain and maintain favorable FBI fingerprint results.

8.9.4.3 Comply with all investigative and adjudicative requirements, including responsiveness to time-sensitive requests (e.g., interviews, additional information, or clarification) from DHRA or DLA Security, a DCSA investigator, or the adjudicative agency.

8.9.4.4 Obtain and maintain favorable eligibility for the Tier background investigation.

8.9.5 Continuous Vetting (CV) for Positions of Trust. In accordance with the DoD Continuous Evaluation (CE) Program and Trusted Workforce 2.0, all personnel must comply with Continues Evaluation (CE) enrollment and re-enrollment requirements upon request to maintain their eligibility.

8.10 Conduct while on Government Installation. The Contractor shall not assign work or direct its employees to access government information, systems, or installations unless the employees possess and maintain the required background investigation, clearances, and authorizations.

8.11 Weapons, Firearms, and Ammunition. Contractor employees are prohibited from possessing weapons, firearms, or ammunition, either in their possession or within their contractor-owned vehicle or privately-owned vehicle, while on any government installation.

8.12 Reporting Requirements. The Contractor shall ensure their personnel are aware of the requirement to report to their supervisor and site security office any information or circumstance they are aware of that may pose a threat to the security of government or contractor personnel, resources, or information.

8.13 Offboarding. Coordination with COR. The Contractor shall coordinate the removal of personnel from work under this contract with the COR upon any of the following occurrences: contract completion, personnel relocation, retirement, resignation, termination, inability to meet contract expectations, or violation of DHRA security policies. In addition, if

any Contractor personnel supporting this contract are unable to obtain or maintain the required security clearance or eligibility, the Contractor shall immediately notify the COR. The Contractor shall remove the individual from roles performed under this contract and replace them with a qualified individual possessing the necessary knowledge, skills, and abilities (KSAs) to perform the services. When offboarding personnel, the Contractor shall:

8.13.1 Utilize DHRA's employee termination checklists, and notification systems, ensuring all relevant parties are informed of the individual's departure.

8.13.2 Retrieving Identification Media. The Contractor shall ensure that all identification media, including vehicle passes and credentials (e.g., CACs, badges, identification cards) is retrieved and returned to the COR, their local Installation Access Control Office, or the Government Security Office.

8.13.3 Ensure issued tokens are returned to the appropriate Certificate Authority (CA) or the respective issuing authority.

Provide an updated list of personnel to the COR within three (3) business days of any change.

9.0 CYBERSECURITY

9.1 Cyber Incident Reporting. In addition to DFARS 252.204-7012, the Contractor shall notify the DMDC Incident Response (IR) team by emailing an initial cyber incident report to dodhra.dodc-mb.dmdc.list.ir-team@mail.mil, the Contracting Officer, and the COR within one hour of discovering any cyber incident. The Contractor shall follow up with a supplemental report every 24 hours until the incident is closed.

9.2 Information System Security. The Contractor shall implement IS security protections that are appropriate for the confidentiality, integrity, and availability needs of the contract. The protections must include the administrative, technical, and physical safeguards necessary to protect all nonpublic Government data.

~~9.2~~9.3 Cybersecurity Maturity Model Certification. The Contractor shall comply with all applicable Cybersecurity Maturity Model Certification (CMMC) requirements in accordance with DFARS 252.204-7021. For the execution of this Performance Work Statement (PWS), the minimum required certification at award is CMMC Level 1. The Contractor must achieve and demonstrate full compliance with CMMC Level 2 (Self-Assessment) within 90 calendar days of contract award.

10.0 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI)

There is no planned distribution of GFP/GFE or GFI during the performance of this contract. Government personnel will be made available to provide technical input, answer questions, review draft deliverables, provide feedback, and provide directions for deliverable products.

11.0 PLACE OF PERFORMANCE

Performance of the tasks required herein shall be at the contractor facilities or at designated military bases. Program discussions and In Process Reviews (IPRs) may be held at Government, designated military bases or virtually.

12.0 QUALITY CONTROL

The contractor shall implement and maintain a Quality Control Plan (QCP) to ensure work performed conforms to the scope of work and meets the requirements under this PWS. The QCP shall, at a minimum, provide a method for performing inspections; identifying, correcting and preventing problems/defective service; addressing customer complaints, and improving the quality of services over the life of the contract.

13.0 QUALITY ASSURANCE

13.1. The Government reserves the right to perform inspections and surveillance to evaluate the Contractor's compliance to the contract terms and performance of the requirements in the PWS.

13.2. Contract Discrepancy Report (CDR). In the event of unsatisfactory contractor performance, the COR or CO will issue a CDR that will explain the circumstances and findings concerning the incomplete or unsatisfactory service. The contractor shall acknowledge receipt of the CDR and respond in writing as to how he/she shall correct the unacceptable performance and avoid a recurrence. The Government will review the contractor's corrective action response to determine acceptability and will use any completed CDR as part of an overall evaluation of Contractor performance when determining present or future contractual actions.

14.0 ORGANIZATIONAL CONFLICTS OF INTEREST

The Contractor acknowledges that it is familiar with FAR Subpart 9.5, Organizational and Consultant Conflicts of Interest, and agrees to avoid, neutralize or mitigate such conflicts of interest in accordance with the principles set forth in the FAR. If the performance requires the Contractor (to include subcontractors) to supply technical support related to systems or projects with which the Contractor is already directly concerned, either by prime or subcontract, the Contractor shall immediately inform the Contracting Officer. The PWS may be withdrawn if a conflict is found. The Contractor shall not undertake performance of any PWS requirements which requires it to supply technical support regarding such systems until the notice is given, and written consent to proceed is issued by the Contracting Officer.

15.0 APPLICABLE DOCUMENTS

Document	Web link
DoD Directive 1322.08 - Voluntary Education Programs for Military Personnel	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/d odd/l 32208p.pdf
DoD instruction 1322.25 - Voluntary Education Programs	https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/d odi/132225p.pdf

16.0 PERFORMANCE REQUIREMENT SUMMARY (PRS)

16.1 Purpose. The PRS lists performance objectives for the required services the Government will surveil. The absence of any contract requirement from the PRS shall not detract from its enforceability nor limit the rights or remedies of the Government under any other provision of the contract.

16.2 Components. The PRS states the performance objective (required service), and threshold (performance standard, accept and reject points (if applicable)) in either a qualitative or quantitative fashion for each critical success factor.

Performance Objective	PWS paragraph	Performance Threshold
System Functionality	4.1	Online tool satisfies system functionality requirements for all users for all engagements.
System Training	4.2.2	Training is conducted when and where scheduled by the COR.
System Availability	4.3.2.	98 percent system availability
Technical Support	4.3.3.	Response to technical support inquiries within 24 hours of receipt (during business hours) and website includes technical support trouble-shooting information.
Reports	4.4	Reports received when scheduled and contain the data prescribed in 4.4.

17.0 Mandatory Training Requirements:

Contractor employees performing under this contract shall complete the following mandatory trainings within 30 calendar days of reporting for duty and annually thereafter when applicable. Refer to the COR/Government point of contact for the websites/links to the specific training identified below. They will provide a sheet with the Mandatory Training Website/links. The Contractor shall provide a copy of its employee(s)' training certificates to the COR/Government point of contact to meet the mandatory training requirements.

1. OPSEC Awareness for Military Members, DoD Employees and Contractors IAW DoDM 5205.02, "DoD Operations Security (OPSEC) Program Manual", dated October 29, 2020.

2. Unauthorized Disclosure of Classified Information and Controlled Unclassified Information IAW DoDI 5200.48, "Controlled Unclassified Information (CUI)", dated March 6, 2020.

3. DoD Mandatory Controlled Unclassified Information (CUI) Training, Executive Order 13556, Controlled Unclassified Information and DoDI 5200.48, “Controlled Unclassified Information (CUI)”, dated March 6, 2020.

4. Insider Threat Awareness IAW DoDD 5205.16, “The DoD Insider Threat Program”, dated August 28, 2017.

5. Privacy Act and Personally Identifiable Information IAW DoDI 5400.11, “DoD Privacy and Civil Liberties Programs”, dated January 29, 2019.

6. IT Security Awareness IAW title 5, Code of Federal Regulations, section 930.301.

7. Counterintelligence Awareness and Reporting Training IAW DoD Directive 5240.06, “Counterintelligence Awareness and Reporting (CIAR)”, dated July 21, 2017.

8. Annual OSD Records and Information Management Training IAW DoD Records Management Program (DoDI 5015.02 Incorporating Change 1, August 17, 2017).