ID CARD SERVICES PERFORMANCE WORK STATEMENT (PWS)

Fort Bragg, North Carolina

29 June 2026
Version: FINAL

PART 1
GENERAL INFORMATION

1. **GENERAL.** This is a non-personnel services contract to provide Defense Enrollment and Eligibility Reporting System (DEERS)/ Real Time Automated Personnel Identification System (RAPIDS) Common Access Card (CAC) support services for the Installation Management Command (IMCOM) at Fort Bragg, North Carolina. The Government will not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

1.1 Description of Services/Introduction. The Contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform the verification and issuance of military identification (USID) and CAC cards for active duty military, Reserve and National Guard members, military retirees, family members, Department of Defense (DoD) civilians and other eligible recipients, as defined in this PWS, except for those items specified as government furnished property and services.

1.2 Background. The DoD CAC is recognized by all DoD components as the official DoD/Federal ID credential that can be used for logical and physical access once access privileges are granted. The CAC also serves as electronic access to secure websites and electronic mail. CAC ID cards are issued to active duty military, Reserve and National Guard members, DoD civilians, DoD Contractors, and other eligible recipients. The DoD also provides USID cards to military retirees, family members, and other eligible recipients. CAC and USID cards are issued and maintained in part using DEERS/RAPIDS workstations. Approximately 79,000 customers are serviced annually in the Soldier Support Center, building number 4-2843 on Fort Bragg. Fort Bragg is located in Cumberland County, North Carolina (NC) and hosts a population of approximately 65,000 military, Government civilian, and contactor personnel, as well as 98,000 resident retirees and family members.

1.3 Scope. This is a non-personal services contract to provide DEERS/RAPIDS USID card and CAC support services for the IMCOM at Fort Bragg, NC. Contractor personnel rendering the services are not subject; either by the contract's terms or by the manner of its administration, to the supervision and control usually prevailing in relationships between the Government and its employees. Contractor employees shall be accountable solely to the Contractor who, in turn, is responsible to the Government.

1.4 Type of Contract. The Government will award a Firm Fixed Price contract.

1.5 Objectives. The Contractor shall provide positive verification and issuance of USID and CAC cards for active duty military, Reserve and National Guard members, military Retirees, Family Members, DoD civilians and other eligible recipients. The Contractor shall perform to the standards specified in this PWS and ensure all work accomplished in the performance of this PWS meets all applicable Federal, State, and local laws, regulations, and directives to include, but not limited to, the publications in PWS Part 6, "Applicable Publications."

1.5 Period of Performance. The period of performance shall be for a thirty (30) day phase-in period, an eleven (11) month base period, and four (4) one year option periods as follows:

Phase-in Period	30 days
Base Period	11 Months
Option Period I	1 Year
Option Period II	1 Year
Option Perion III	1 Year
Option Period IV	1 Year

1.6 General Information.

1.6.1 Quality Assurance. The Contracting Officer's Representative (COR) will evaluate the Contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused on what the COR must do to ensure that the Contractor has performed IAW the performance standards and contract quality requirements are being met. Contract quality requirements means the technical requirements in the contract relating to the quality of the product or service and those contract clauses prescribing inspection, and other quality controls incumbent on the Contractor, to ensure they are providing products or services that conform to the contractual requirements. It defines how the performance standards will be enforced, the frequency of surveillance, the minimum acceptable defect rate(s), and deductions applied, if applicable. When an observation indicates defective performance, the COR will require the Contractor or designated on-site representative to initial the observation to acknowledge the defective performance. The acknowledgement of the observation does not necessarily constitute Contractor concurrence with the observation, only that the Contractor acknowledges that they have been made aware of the defective performance.

1.6.1.1. Quality Control Plan (QCP). Quality Control is the responsibility of the Contractor. The Contractor is responsible for the delivery of quality services and supplies to the Government The Contractor shall develop, implement, and maintain a QCP to provide delivery of high-quality service and products IAW the requirements of the contract, applicable laws and regulations, and at or above the standards defined in the Performance Requirements Summary (PRS).

1.6.2. Inspection Files. The Contractor shall keep records on-site of all inspections conducted by the Contractor and necessary corrective action taken. Upon request from the KO or COR, the Contractor shall provide, all reports generated as a result of the Contractor's quality control efforts. This shall include any summary information used to track quality control, including any charts/graphs.

1.6.3. COR/Alternate COR (ACOR): The COR and ACOR monitor all technical aspects of the contract and assists in contract administration. As determined by the KO, a COR and ACOR will be identified and appointed by letter of designation, a copy of which will be provided to the Contractor by the KO. The designation letter states the responsibilities and limitations of the COR and ACOR, especially regarding changes in cost or price, estimates, or changes in delivery dates. The ACOR's authority shall only be in effect during the absence of the COR.

1.6.3.1. In no event will the COR or ACOR, by virtue of their designation as such, be empowered to execute or agree to any contract changes thereof or authorized to obligate the Government. If the work is not written in the contract, neither the COR nor ACOR are authorized to request new work. The KO retains the ultimate responsibility for the administration of the contract. Any discrepancy resulting from coordination with or advisement from the COR or ACOR shall be addressed, in writing, to the KO.

1.6.3.2. The COR and ACOR are authorized to perform the following functions: Assure that the Contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; and maintain written and oral communications with the Contractor concerning technical aspects of the contract. The COR and ACOR can also issue written interpretations of technical requirements, including government drawings, designs, and specifications; monitor Contractor's performance; notify both the KO and Contractor of any deficiencies; coordinate availability of government furnished property; and provide site entry of Contractor personnel.

1.6.4. Corrective Action Request (CAR). Nonconformance occurs when a Contractor fails to meet Contract or Task Order terms, conditions and/or specifications; the Contractor's quality control system is found to be inadequate; or the Contractor's noncompliance has led to substandard performance requiring corrective action. All instances of nonconformance will be documented via a Corrective Action Request. The Contractor shall reply to the KO within the due date established in the issued CAR, giving the reasons for the unsatisfactory performance, corrective action taken, and procedures to preclude recurrence. A CAR will not normally be issued if the Contractor has self-identified a nonconforming condition and has

implemented effective corrective actions. However, this does not apply in cases where a Contractor has issued an internal corrective action based on a nonconformance previously identified by the Government.

1.6.5 Recognized Federal Holidays. Contractor services are not required on the Federal public holidays listed below. Holidays occurring on weekends will be observed as directed by the Federal calendar (5 U.S.C. 6103).

New Year's Day
Birthday of Martin Luther King Jr.
Washington's Birthday
Memorial Day
Juneteenth Day
Independence Day
Labor Day
Columbus Day
Veterans Day
Thanksgiving Day
Christmas Day

1.6.6 Regular Hours of Operation. The Contractor shall work on the days the Government is scheduled to work. The Contractor is responsible for conducting business, between the hours of 0800 - 12:00 and 13:00 – 17:00 hours, Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government-directed facility closings. The Contractor shall conduct business during regular hours unless a mission requirement necessitates extended hours of operation in accordance with PWS paragraph 1.6.6.1. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

1.6.6.1 Extended Hours of Operations. Due to mission requirements such as deployments and redeployments of units, there are occasions during which the Fort Bragg ID Card Facilities may need to operate for extended periods before or beyond regular hours of operation, including Federal Holidays. In these instances, the Government will notify the Contractor at least 24 hours in advance to allow the Contractor time to rearrange work schedules leading up to the event and avoid the need for overtime. The Contractor will be authorized to provide a flexible work schedule for its employees who are required to work extended hours on those days in order to meet mission requirements. Prior to performance of services outside the regular hours of operation, the Contractor shall request and obtain, in writing, approval from the Contracting Officer (KO).

1.6.6.2 Installation Closures. When an unforeseen installation or directorate closure occurs on a regularly scheduled day of work, the Contractor shall resume operations on the next business day that the facilities are open.

1.6.6.3 The Contractor shall ensure an adequate workforce is in place for uninterrupted performance of all tasks defined within PWS Part 5 during the hours of operation detailed in this PWS.

1.6.7 Place of Performance. The work implemented under this contract will be performed at the following location:

Soldier Support Center (SSC)
Building 4-2843. Normandy Drive
Fort, Bragg, NC

1.7 Security Requirements. Contractor personnel performing work under this contract shall have and maintain a favorable National Agency Check with Inquires (NACI) at the time of their performance start date and for the duration of their performance under the contract.

1.7.1 Physical Security. The Contractor shall be responsible for safeguarding all government equipment, information and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

1.7.2 Key Control. The Contractor shall establish and implement methods of making sure all keys/key cards issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to the Contractor by the Government shall be duplicated. The Contractor shall develop procedures covering key control that shall be included in the QCP. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The Contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the KO.

1.7.2.1. In the event keys, other than master keys, are lost or duplicated, the Contractor shall, upon direction of the KO, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks will be deducted from the monthly payment due the Contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government and the total cost deducted from the monthly payment due the Contractor.

1.7.2.2. The Contractor shall prohibit the use of Government issued keys/key cards by any persons other than the Contractor's employees. The Contractor shall prohibit the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the KO.

1.7.3 Lock Combinations. The Contractor shall establish and implement methods of ensuring that all lock combinations are not revealed to unauthorized persons. The Contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the Contractor's QCP.

1.7.4 For contractors that do not require CAC but require access to a DoD facility or installation. Contractors and all associated sub-contractors employees shall be screened using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05/AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative), or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations. Contractors or Contract Leads will coordinate with the COR to receive an entry badge (AIE). All issued badges will not exceed the issuance of three years or the length of the contract. Contractors requiring access to the installation will go to the visitor center to obtain a badge of access. Contractors will turn in the badge to the COR upon expiration of the contract or separation from the contract. Lost, damaged, or stolen badges will be reported immediately to the COR. IAW AR 190-51, at no point will a contractor use a retiree, or other DoD ID to access the installation unless it is a CAC ID, issued by the US Government and sponsored locally.

1.7.5. Operations Security (OPSEC) Requirements: Contractor personnel shall adhere to facility security policies and restrictions. The Contractor shall immediately report suspicious activities to security personnel.

1.7.6 <u>Special Qualifications</u>.

1.7.6.1 Security.

1.7.6.1.1 Access and General Protection/Security Policy and Procedures. The Contractor and all associated subcontractors' employees shall comply with applicable installation, facility, and local security policies and procedures. The Contractor workforce shall comply with all personal identity verification (PIV) requirements as directed by DoD, Headquarters Department of the Army (HQDA), and local policy. The Contracting Officer's Representative (COR) and/or Alternate COR (ACOR) will request changes in Contractor security matters or processes if the Force Protection Condition (FPCON) at any individual facility or installation changes.

1.7.6.1.2 The Contractor shall provide all information required for background checks to meet installation access requirements, to be accomplished by the installation Provost Marshall Office, Director of Emergency Services, or Security Office.

1.7.6.1.3 The Contractor shall return CAC cards the same day employment of an individual has expired or has been terminated and shall return them to the issuing office within one day.

1.7.6.1.4 The Contractor shall immediately report any lost or stolen CAC or government issued identification cards to the COR and Military and/or DoD police agencies. The Contractor shall immediately collect the CAC and other government issued forms of identification upon termination of employee, or at the end of the contract performance period. The CAC and other government issued forms of identification (e.g., badges) shall be returned to the COR within one (1) hour of employee termination or at the end of contract performance period, whichever comes first. Final payment may be delayed if Contractor fails to comply with these requirements.

1.7.6.1.5 Physical Security. The Contractor shall safeguard all Government equipment, information, and property provided for Contractor use. The Contractor shall maintain a physical security checklist or log (e.g., Standard Form (SF) 701, Activity Security Checklist), which shall be forwarded to the KO and COR/ACOR, no later than the fifth working day of each month following the month of surveillance. The Contractor shall secure Government facilities, equipment, and materials at the close of each work period. The Contractor shall be solely responsible for any loss or damage of equipment and material. The Contractor shall ensure debris of any type is disposed of according to local policies and directives.

1.7.6.2 Security Training

1.7.6.2.1 iWATCH Training. The Contractor shall brief the local iWATCH program training to all Contractor personnel and associated subcontractors. Training standards will be provided by a Government Anti-Terrorism Officer (ATO). This training is used to inform employees of types of behavior to watch for and instructs employees to report suspicious activity to the COR/ACOR. The Contractor shall furnish, to the KO and COR, certificates of completion for each employee no later than 30 days after the performance start date and annually thereafter.

1.7.6.2.2 Anti-Terrorism Training. The Contractor shall complete Anti-Terrorism Training available at https://jkodirect.jten.mil/. The Contractor shall furnish, to the KO and COR, certificates of completion for each employee no later than 30 days after the performance start date and annually thereafter.

1.7.6.2.3 Level 1 OPSEC training. The Contractor shall complete the training within thirty (30) calendar days of contract performance start date and within five (5) calendar days of new employees commencing performance. Contractor employee training status shall be reported to the KO and COR/ACOR no later than thirty (30) calendar days after contract performance start date. Contractor personnel shall complete OPSEC awareness training annually at https://jkodirect.jten.mil/.

1.7.6.2.4 DoD Cyber Awareness Training. All Contractor personnel with access to a government information system shall be registered in the Army Training Certification Training System (ATCTS) at contract performance start date, and must successfully complete the DoD Information Assurance Awareness training prior to accesses the information systems and then annually thereafter. A certificate of completion shall be furnished to the KO and COR during Phase-in and annually thereafter, no more than 30 days prior to expiration.

1.7.6.2.5 Threat Awareness Reporting Program. Per 2-4b of AR 381-12 Threat Awareness and Reporting Program (TARP), Contractor personnel shall receive live TARP training by a Counterintelligence (CI) agent or other trainer and annually thereafter as specified in 1-10b and 1-10l of AR 381-12.

1.8 Safety

1.8.1 The Contractor shall comply with AR 385-10, *The Army Safety and Occupational Health Program* and adhere to Occupational Safety and Health Administration (OSHA) standards and all applicable Federal, State, and local laws, regulations, and directives. Provide a verbal notification to the KO as soon as possible of each occurrence of damage to Government property or an accident resulting in death, injury, occupational disease, or adverse environmental impact.

1.9 Contingency Plans.

1.9.1 The Contractor shall establish, maintain, and implement contingency plans for mobilization, disaster, and labor dispute contingencies. The plans shall assume no Government support to the Contractor workforce. The Contractor shall, within thirty (30) days of contract performance start date, designate in writing to the KO and COR, a single point of contact to be the Designated Contingency Coordinator (DCC) within the Contractor's organization. The DCC shall coordinate with the COR to participate in the installation contingency and mobilization planning activities. The DCC, through coordination with the COR, shall participate in the local installation mobilization planning and execution conferences and shall modify and maintain appropriate Contractor contingency plans to compliment or enhance corresponding installation plans. No travel will be required for the planning activities and conferences referenced in this paragraph.

1.10 Mission Essential Services.

1.10.1 The Government has identified all of the contractor services performed under this contract as essential contractor services that must be executed during emergency and/or crisis events. All tasks listed in PWS Part 5, Specific Tasks, are mission-essential functions. Mission-essential functions means those organizational activities that must be performed under all circumstances to achieve DoD component missions or responsibilities. Failure to perform or sustain these mission essential functions would significantly affect DoD's ability to provide vital services or exercise authority, direction, and control. The Contractor shall maintain and update the Mission-Essential Contractor Services Plan in accordance with DFARS Clause 252.237-7023, as necessary. Any changes made to the Mission-Essential Contractor Services Plan shall be submitted to the COR and KO no more than 10 days prior to implementation.

1.11 <u>Post Award Conference/Periodic Progress Meetings.</u> The Contractor shall attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The KO, COR, and other Government personnel, as appropriate, may meet periodically with the Contractor to review the Contractor's performance. At these meetings the KO will apprise the Contractor of how the Government views the Contractor's performance, and the Contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the Government.

1.11 <u>Contracting Officer (KO).</u> The KO is the only person authorized to direct changes in any of the requirements under this contract, and, notwithstanding any provisions contained elsewhere in this contract, said authority remains solely with the KO. In the event the Contractor makes any change at the direction of any person other than the KO, the change shall be considered to have been made without authority and solely at the risk of the Contractor. Communications pertaining to contract administration matters shall be addressed to the KO. No changes in or deviation from the terms and conditions shall be affected without a written modification to the contract, executed by the KO, authorizing such changes.

1.12 <u>Contracting Officer Representative (COR)/ Alternate COR</u>. The COR will be identified by separate letter. The COR and ACOR monitors all technical aspects of the contract and assists in contract administration. The COR and ACOR are authorized to perform the following functions: ensure that the Contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; maintain written and oral communications with the Contractor concerning technical aspects of the contract; issue written interpretations of technical requirements, including Government drawings, designs, specifications; monitor Contractor's performance and notify both

the KO and Contractor of any deficiencies; coordinate availability of government furnished property (if required), and provide site entry of Contractor personnel. A letter of designation issued to the COR and ACOR, a copy of which will be sent to the Contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR and ACOR are not authorized to change any of the terms and conditions of the resulting contract.

1.13 Key Personnel. The following personnel are considered key personnel by the government: Program Manager (PM) and Site Security Managers (SSM).

1.13.1 Program Manager (PM): The Contractor shall provide a contract PM who shall be responsible for the performance of the work. The name of the PM who shall act for the Contractor when the PM is absent, shall be provided in writing to the KO on the first day of the Phase-in period. The PM shall have full authority to act for the Contractor on all matters relating to daily operation of this contract. The PM shall be available during regular hours of operation as defined in PWS paragraph 1.6.4. Qualifications for the PM are as follows: The PM shall be able to understand, speak, read, and write the English language. Historically the PM is not located at Fort Bragg NC 28310 and resides at the location of the awarded contractor.

1.13.2 Site Security Managers (SSMs): Serves as the manager for a specific ID card facility. The SSM performs all roles of the VO plus represents the site as the Subject Matter Expert (SME) for DEERS and ID Card policy and procedures. The SSM contacts DMDC and/or APO for elevated DEERS and ID card issues, installs hardware components, troubleshoots equipment and software issues, manages and trains site users, ensures the security of cardstock, consumables, and equipment, runs, and reviews audit reports, and maintains the site's information for the RAPIDS Site Management Tool (SMT). The SSM also performs RAPIDS security overrides for document and fingerprint support. To perform these responsibilities, the SSM uses Security Online, Inventory Logistics Portal (ILP), Statistical Analysis Software (SAS), SMT, RAPIDS Configuration Tool, and the VOIS. Other requirements of an SSM include:
a. An ID card facility is required to have two RAPIDS certified SSMs always assigned to the site. It is the site's responsibility that a new SSM is added to the site and RAPIDS certified before an SSM departs.
b. SSMs are responsible for:
(1) User administration and user security
(2) Cardstock and consumables: ordering, management, and accountability
(3) Policy and procedure compliance
(4) Site administration and security
(5) Documentation and training
(6) Installation of hardware components
(7) Validation of the identity of individuals whose fingerprints cannot be captured.
(8) Document overrides in the event a CAC recipient does not have proper identification documents.
c. SSMs must:
(1) Be accountable for maintaining all RAPIDS workstation hardware components. Perform regular maintenance and upgrades to improve equipment functionality and efficiency. All activities to include relocating the RAPIDS hardware must be coordinated through the APO and approved by DMDC. If a site fails to properly follow guidance and inventory is lost, stolen, or misplaced, the site will be responsible for providing funds to DMDC to replace items.
(2) Make sure to receive, accept, and open cardstock shipments in the ILP before attempting to issue them. Keep on-hand cardstock count up-to-date and report any discrepancies using the Cardstock and Consumables Order Form. SSMs can find the order form on the VOIS.
(3) Return all CACs and USID Cards to DMDC. This includes cards that are returned by customers, security officials and HR personnel.
(4) Manually request emergency CAC/USID card shipments and consumables.
(5) Ensure that the RAPIDS system is included in their local Continuity of Operations Plan (COOP). Utilize the RAPIDS COOP Template posted on the VOIS.
(6) Access the RAPIDS Configuration Tool to install new or replacement hardware devices.
(7) Add, Change, or Delete VOs in Security Online.

(8) Keep up with all RAPIDS/DEERS/ID card policies and procedures and ensure personnel, to include the installation community, is aware of changes pertinent to them. Monitor the VOIS website daily to receive new Messages of the Day (MOTD) and DMDC newsletters.
(9) Read and disseminate the quarterly Army Project Office Digest to site personnel.
(10) Ensure SSMs and VOs sign the DD Form 2841 to fulfill their LRA responsibilities for issuing an identity or network credential, reflecting PKI certificates to the card receipt. The DD Form 2841 is maintained locally by the SSM.
(11) Ensure RAPIDS hardware custody and accountability. DMDC maintains custody and accountability of RAPIDS hardware and supporting software. The SSM keeps the DD Form 1149 Requisition and Invoice/Shipping Document on file for equipment inventory, including taking measures for accountability of equipment during staff turnover. Note: RAPIDS facilities are custodians of DMDC hardware/software assets by controlling, supervising, and managing the property in their care as listed in DoDI 5000.64, Accountability and Management of DoD-Owned Equipment and Other Accountable Property. RAPIDS equipment life cycle requires replacement due to use, new and emerging technologies. When the RAPIDS equipment is no longer in use (life cycle is complete), return the equipment to DMDC.
(12) Ensure physical security and must maintain the RAPIDS platform as provided. DMDC prohibits altering of RAPIDS hardware configurations and software modifications, including, placing alternative boot/reboot media, or connecting non-approved external storage media devices, and unauthorized moving of equipment. Note: RAPIDS facilities who fail to follow published guidance and inventory is lost, stolen, damaged, or misplaced are responsible for replacement costs to DMDC.
(13) Ensure proper security and access control by ensuring users at the site:
(a) Keep their CAC and PIN secure.
(b) Make sure that the user who is logged in to the RAPIDS workstation is the only one completing transactions in RAPIDS.
(c) Make sure the workstation monitors face away from the customer and that a privacy screen is used.
(d) Ensure that there are sound barriers around the workstation to protect audible data exchange with customers.
(e) ALWAYS remove their CAC from the card reader when leaving the RAPIDS workstation. If leaving the RAPIDS workstation for long periods, log off the workstation so that the next person can log on. Always keep your CAC with you.
(f) Store all cardstock (used, unused, failed, and confiscated), and consumables in a locked drawer/cabinet/safe away from customer view or unauthorized access, during and after duty hours. Secure RAPIDS equipment in a locked area after duty hours.
(g) Allow only DMDC authorized software and hardware to be installed on the RAPIDS workstation.
(14) Ensure that during ID card issuance:
(a) Make sure the background behind the customer is solid white and does not display any patterns, symbols, etc.
(b) Site users educate customers about the CAC. Request that the customer read the posted DD Form 2842, Acknowledgement of Responsibilities, as being a CAC holder. Before issuing an ID card, the customer will have to agree to the terms of the DD Form 2842 by digitally signing this document. Be sure the customer is aware they are signing a legally binding document.
(c) The customer and RAPIDS operator remain at the workstation during the entire CAC issuance process.
(d) Site users provide the customer with a DMDC issued CAC protective sleeve and instruct them to keep their CAC in the sleeve or a plastic cardholder to protect it from damage. The customer should not place stickers on, write on, stamp, or punch holes in their CAC.
(e) Site users write the correct error code on CACs that fail during issuance or CACs that are confiscated. A full list of ID Card Error Codes is available on the VOIS.
(15) Ensure proper RAPIDS Workstation Maintenance:
(a) Always keep the Virtual Private Network (VPN) connected on the RAPIDS workstation to allow for software updates. For more information on how to sustain VPN connection on workstation(s), see the VPN Connectivity Tip Sheet on the VOIS.

(b) Maintain the fingerprint scanner by wiping it down after every use with a dry lens cloth. Do NOT use any alcohol-based substances to clean the platen.
(c) Clean the Smart Card printer regularly to reduce the frequency of printer failures and ensure that the printer is operating efficiently to produce high quality cards. Refer to the Printer Cleaning Instructions on the VOIS.
(d) Because Smart Card printer consumables have a shelf life of 12-18 months, sites should practice the first-in, first-out inventory methodology. Mark the outside of the consumable's package with the date received and use the oldest consumables first.
(e) Destroy the Smart Card printer ribbon and transfer film that contains PII. The Privacy Act protects PII. Dispose of the printer consumables in accordance with local security procedures (i.e., shredding). The APO does not recommend burning the ribbons because the materials will emit hazardous gases. Refer to the Proper CAC Printer Ribbon and Re-transfer Film Disposal/Destruction Policy on the VOIS.
(f) Sites must install any shipped maintenance replacement components within 3 days of receipt and return the component needing repair to the maintenance vendor, using the prepaid shipping label that accompanies the replacement equipment.
d. The verification of the Primary and Secondary fingerprint may be necessary if the VO cannot successfully match an individual's fingerprint or when the beneficiary is not present. The SSM can perform the skip fingerprint verification when a person's identity can be verified through another means or is already positively identified.
e. For high-volume Common Access Card Central Issuance Request Station (*CACCIRS*) sites:
(1) Prior to creating a Central Issuance Facility (CIF) request on a CACCIRS workstation, the SSM must establish a Person in Charge (PIC) who will be responsible for CAC distribution. Once the PIC has been identified, the SSM must add the PIC to the site PIC list in RAPIDS.
(2) Proper security procedures dictate that one SSM receives the CACs and a different SSM receives the PIN mailer shipments. For the most up-to-date information about CACCIRS sites, SSMs should refer to the ILP User Guide located on the VOIS. Failure to receive the CACs or PINs, as well as failure to accept the CACs in the ILP, prevents CAC recipients from accessing a DoD network.

1.13.2.1 SSM Specific Responsibilities.
a. SSM Applications. SSMs will utilize the following applications to fulfill their duties:
(1) Security Online. SSMs perform all user administration functions through Security Online, which include adding a user to a site, assigning roles to a new user, updating user information, deactivating a user, and managing site information.
(*a*) SSMs are responsible for verifying with their appropriate command security office the appropriate vetting has been initiated on behalf of a VO. Once verified, a VO can be added to the site roster via the Security Online application.
(*b*) After adding a new user to the site, the SSM is responsible for assigning roles that provide a user with access or privileges. The SSM can only assign the roles of a VO and cannot assign the roles of SSM. A The APO must endorse the request to assign SSM roles. If the SSM assigns a new VO role, they must ensure they meet security requirements to access RAPIDS. The SSM will need to assign the following roles to VOs to issue Common Access Cards (CACs):
1.Issuing Official (IO) – verifies data and issues ID cards but cannot enter data into DEERS
2. Verifying Official (VO) – verifies or authenticates the registered individual against the DEERS database.
3. Local Registration Authority (LRA) – entity authorized by a RA to verify subscribers' identity and collect information for public key certificates, and to forward requests for certificates to the CA.
(*c*) The Security Online application also provides the SSM with the capability of reviewing the contact information and roles assigned to all RAPIDS users associated with the site. In addition, the Security Online application will allow the SSM to monitor the training courses of all RAPIDS users.
(*d*) The SSM administrative responsibilities include updating contact information for their site. Keeping site information current is important to an ID Card facility because DEERS shares this information with other systems that are critical to the installation, maintenance, and support of RAPIDS. SSMs update the site contact information, which includes site mailing address, site location address, and site telephone numbers using Security Online.

(2) RAPIDS Device Configuration Tool. Provides a way for SSMs to install and configure components for the RAPIDS workstation. The SSM accesses this tool by clicking the RAPIDS Configuration icon on the RAPIDS desktop.
(3) Inventory Logistics Portal (ILP). Tool designed to track CAC and USID cardstock and automate the CAC/USID reorder process. The ILP automatically reorders CAC/USID cardstock based on the reorder threshold and reorder quantity specified for each site.
(*a*) There is 100 percent accountability at RAPIDS sites for CACs. All CACs are accounted for by the DMDC. ILP helps SSMs accomplish this.
(*b*) The ILP has three main functions:
1. Monitors and orders CAC cardstock based on the site's inventory levels, card issuance rates, and assigned reorder threshold
2. Continuously updates the individual card status; options include Available, Issued, and Terminated
3. Tracks cardstock and consumables shipments
(4) Statistical Analysis Software (SAS). Using SAS, SSMs can access, run, customize, manage, save, and print RAPIDS reports. SAS helps SSMs manage security, technical and training issues at their site, as well as monitor cardstock and workload management. Using RAPIDS reports generated in SAS, SSMs will be able to track card transactions for CACs and USID cards issued from an ID card facility.
(*a*) SAS provides capabilities for reporting to include:
1. Ability to choose from three options to view, export and print reports
2. Ability to access RAPIDS reports from a CAC-enabled, non-RAPIDS workstation using a web browser
3. Ability to produce report output in various formats, including output type PDF and Excel. Note: Excel format is only available to view on a CAC-enabled, non-RAPIDS workstation
(*b*) RAPIDS reports should be run and reviewed by SSMs daily and weekly to help identify security, technical, or training issues at the ID card facility. After viewing daily reports, SSMs should consolidate report data by viewing a weekly report, which should replace the individual daily reports. At the end of each month, a monthly report should be run to replace the individual weekly reports. Quarterly reports should be run to replace the individual monthly reports. Once the daily, weekly, and monthly reports have been consolidated into a quarterly report, they can be deleted.
(5) Verifying Official's Information System (VOIS). The VOIS provides real-time systems information, updated program information, and many other resources, such as archived MOTDs, points of contact (POC), RAPIDS documentation, and links to other Websites.
(*a*) RAPIDS users can access the VOIS from either a RAPIDS workstation or a CAC-enabled non-RAPIDS workstation. Please review each link to familiarize yourself with all the resources available to you on the VOIS.
(*b*) Below is a list of the significant documents in each section:
1. Policy—Separated into two sections:
a) DoD and Service-level Policy— DoDI 1000.13, DoDM 1000.13 v1 and v2
b) Supporting Memorandums—Memorandums from the Defense Human Resource Activity (DHRA)
2. RAPIDS User Guide—RAPIDS User Guides, Features and Enhancements (F&E) documents
3. Training Aids—Broken down into the following sections:
a) Tip Sheets – Procedures on performing various tasks within RAPIDS
b) DMDC Learning Site—DMDC LMS User Guide, Web-Based Training (WBT) Matrix, WBT Memo,
c) Posters & Flyers – How to Return CACs to DMDC flyer
d) Best Practices – Document Scanning Best Practices
4. Newsletters—Did You Know Newsletters
5. Hardware – Information on the Smart Card Printer, Camera, Fingerprint Scanner, Other Peripherals, Laser Printer, Desktop/Deployable/Shipboard System
6. Forms—Gives the user access to all the documentation and instructions regarding CAC issuance and ordering CAC consumables, including DD Form 1172-2, DD Form 2841, DD Form 2842, and the Cardstock and Consumables Order Form.
7. Security— Privacy Act Statement, Security Standard Operating Procedures (SSOP) for RAPIDS, RAPIDS Continuity of Operations (COOP) Planning Checklist
8. RAPIDS Related Applications—RAPIDS Site Locator, Mil Connect, DMDC RAPIDS Reporting Tool
9. Contacts—Help Desk Contact Centers, Service Project Officers (SPO), TASS Service and Agency SPOCs, Medical Project Officer List
10. Links—CAC.mil, Defense Health Agency, Other Resources

11. Messages of the Day (MOTD)
a) Presents the user with the current MOTD
b) Allows the user to view an archive of old MOTDs
12. What's New—Documents that have been posted within the past 30 days
13. System Status
a) Provides an updated status diagram and table of the DMDC Network
b) Lists projected/scheduled outages
b. Managing Supplies in the ILP. The SSM must register the cardstock before using the media to create ID cards. To register the cardstock, the SSM must "Receive," "Check," "Accept," and "Open" the cardstock. If the SSM does not perform these operations on each new shipment of cardstock, the media will not be able to complete the issuing process. For detailed procedures and guidance on how to Receive, Check, Accept, and Open the cardstock, please reference the ILP User Guide. The ILP User Guide can be located on the VOIS.
(1) If there is a need for an out-of-cycle ordering of cardstock or consumables, fill out the Cardstock and Consumable Order Form located on the VOIS and send the request to the APO explaining why you need an additional shipment.
(2) If you are manually ordering cardstock because of a discrepancy with the count of cardstock on hand versus the count in the ILP, identify the discrepancy in Section II of the Cardstock and Consumables Order Form. The APO reviews cardstock discrepancies against transactions.
(3) The Chip Unique ID (CUID) is the alphanumeric ID located in the upper right-hand corner on the back of the CAC. If the SSM enters an incorrect CUID, it will cause card count discrepancies in the ILP. These discrepancies are due to incorrect card statuses in the ILP. SSMs may need to manually input a CUID when the card reader cannot read the chip on the CAC. Inputting a CUID is a monitored activity. Failure to support this will result in continued on-hand reporting in the ILP.
(4) Reporting missing CAC/USID Cardstock. SSMs at each site are responsible for the proper management of all cardstocks sent to their site. If, despite all precautions, cardstock is missing the following actions must be taken:
(*a*) The SSM performs all due diligence to locate the missing cardstock (e.g., confirms tracking number, date of delivery, and signature of person who signed; and verifies that the cardstock is not in the mail room or other location on the base).
(*b*) If the cards cannot be located, the SSM reports the missing shipment to the APO.
(*c*) The APO contacts DMDC Customer Operations regarding the missing cardstock and initiates a formal investigation.
(*d*) DMDC marks the shipment as temporarily lost in the ILP. DMDC may provide cardstock support while the investigation is underway.
(*e*) The SPO provides a final report to DMDC Customer Operations. The report must include the following:
1. Details regarding the steps taken to locate the missing cardstock
2. Actions taken to prevent future cardstock losses
(*f*) DMDC reviews the report for completeness and notifies the SPO of the next steps to take.
1. If the report is satisfactory, DMDC marks the shipment as permanently lost in the ILP and removes it from the site's inventory. Normal processing resumes.
2. If the report is unsatisfactory, DMDC requests additional information from the SPO. Additional actions may be required if mishandling of cardstock reoccurs at the site.
c. Returning CAC/USID Cardstock.
(1) Failed, rejected, or returned ID cards contain information regarded as Privacy Act and PII and must be returned to DMDC by FedEx using the DEERS/RAPIDS FedEx account number.
(2) DMDC monitors the FedEx account regularly. Sites should only use it for the return of cardstock. When using this number, your site will not incur shipping costs. DO NOT destroy, shred, or cut ID cards. RAPIDS operators are responsible for safeguarding ID cards by keeping them locked in a secure drawer, cabinet, or safe at your site until returned to DMDC for destruction. DMDC has a 100% accountability requirement for ID cards, so return all ID cards to DMDC for final destruction using the provided information below.
(3) SSMs must ensure that unauthorized persons do not obtain ID cards at sites by becoming familiar with the controls for processing and handling. SSMs should also inventory ID cards monthly or whenever an issuing officer is relieved of custodial duties.

(4) The DEERS database and RAPIDS application maintain security by linking the SSN of the sponsor to the type of card issued. For additional security, the DEERS database maintains a 4-digit alphanumeric security code, which is not visible to the user.
(5) As required by the Privacy Act of 1974, all returned cardstock should be double packaged for return to DMDC to protect the PII displayed on the printed ID card.
(*a*) The first (inner) package should be a large brown envelope or box marked "For Official U.S. Government Use Only". The inner package should contain the returned CACs, a cover sheet stating the number of ID cards, site ID, and site contact information, and the Privacy Act Data Cover Sheet, which identifies the cardstock as containing PII data.
(*b*) The second (outer) package should be a box from Federal Express or from your site. Insert the first (inner) package into the second (outer) package for return shipment using the FedEx account provided by DMDC or by an approved traceable means; in the rare instance your location cannot access FedEx shipping support.
(*c*) Inspect the outer box to ensure that it is in good condition and can be properly sealed. There should be no markings on the outer box. The box must be able to withstand the weight of the cardstock and should not break when in transit. If a box breaks or opens in transit, you risk exposing PII data contained on the returned ID cards.
(*d*) ID cards contain Privacy Act data, and it is your responsibility to ensure that a Privacy Act Data Cover sheet is included in the package. The Privacy Act Data Cover Sheet is in the Chapter 18: Appendices. Print the Privacy Act Data Cover Sheet in color.
(*e*) Complete Section 1, including a commercial telephone number.
(*f*) Complete Section 3:
1. CAC Consumables Team,
2 (800) 372-7437 Defense Manpower Data Center
3. 2102 E. 21st Street N
4. Wichita, KS 67214
(*g*) Under Section 4a, check the FedEx Express Saver checkbox.
(*h*) Under Section 7, Payment, check the Third-Party checkbox and enter the following FedEx Account number: 2283-7326-5
(*i*) Include a cover sheet specifying the number of returned ID cards, your Site ID, and the contact information for your Site.
(*j*) Place returned ID cards and the Privacy Act Data Cover Sheet into a FedEx envelope or package marked "For Official Government Use Only".
(*k*) Affix the FedEx US Air bill to the package and arrange for pickup or drop off.
(*l*) Remove and retain the back copy of the FedEx US Air bill (labeled Recipient's Copy) for your records.
Note: SSMs should use the FedEx account number above to return cardstock only. DMDC regularly monitors this account. If you have further questions, please contact the DSC User Help Desk.
(6) For more information on returning cardstock and CACs, refer to the ILP User Guide on the VOIS.
d. Handling and Safeguarding of Cardstock and Consumables.
(1) As an SSM, you are responsible for safeguarding your site's cardstock. Whenever you receive new blank cardstock, keep it in the factory shrink-wrapped package, locked in a secure drawer, cabinet, or safe at your site until it is loaded into the ID card printer. Once loaded into the printer, do not remove the cardstock. Cardstock may remain in the printer when not in use for short periods (e.g., overnight) if the printer is properly safeguarded from unauthorized access. Sites are responsible for safeguarding their cardstock. A locked office door with limited access to authorized personnel is an example of safeguarding cardstock.
(2) Used printer consumables contain information regarded as Privacy Act and PII. The printer ribbon and transfer film contain information that is printed on the cardstock produced in the Smart Card printer. It is important that sites destroy or properly dispose the printer ribbon and transfer ribbon...
(3) Remove cardstock media and printer consumables before shipping the Smart Card printer. It is important to keep all printers in good working order by performing routine maintenance as required by the DMDC. At times, it will be necessary to remove the printer from your facility for repairs. You are responsible for removing any printer color ribbons, transfer film, laminate rolls, cardstock, and toner cartridges from the printer prior to sending the printer in for repair, maintenance, or long-term storage. During any time between sending a printer for repair and awaiting return instructions, all printer consumables must remain locked in a secure drawer, cabinet, or safe at your site. It is okay to leave

cardstock and consumables in the printer when not in use for short periods of time (e.g., overnight) if you properly safeguard the printer from unauthorized access.
(4) Properly storing, caring for, and securing cardstock media and related consumables is necessary to ensure the best quality printing of ID cards. Consumables have a shelf life of 12–18 months. Cardstock has a shelf life of 3 years.
(5) Along with each CAC cardstock shipment, you should receive electromagnetic sleeves (EMS) for distribution to CAC recipients. The sleeves are to be provided to the CAC recipient customer to shield the contactless interface from unauthorized access as mandated by Federal Information Processing Standards (FIPS) 201-3 Personal Identity Verification (PIV) of Federal Employees and Contractors. EMS shipments will be tracked within the ILP like printer consumables shipments.
e. RAPIDS Equipment Relocation Policy. Relocating the RAPIDS hardware must be coordinated through the APO and approved by DMDC. If a site fails to properly follow guidance and inventory is lost, stolen, or misplaced, the site will be responsible for providing funds to DMDC to replace items. DMDC does not support altering of the hardware or software configuration. External devices should not be connected to the RAPIDS workstation, to include USB drives and any additional hardware components not provided or authorized by DMDC.
(1) Submit a request for a self-help relocation move to the APO the Workstation Relocation Request Form located on the VOIS.
(2) The APO will forward the request to DMDC for review and action. Once approved, DMDC will contact the site directly for coordination of the move.
f. Continuity of Operations Plan (COOP). SSMs will establish written procedures to identify measures to provide uninterrupted service for the local customer base and provide a quick return to operation after a system failure. If there is a systems failure or power outage, the SSM should consider the following for COOP:
(1) For short-term outages of 3 days to 1 week, give customers information of other RAPIDS Issuing Facilities within the local commuting area (up to 60 miles).
(2) For outages estimated to last for more than 10 days, SSMs may consider requesting relocation for RAPIDS hardware through the APO. The COOP Template is available on the VOIS.
g. Disposition of RAPIDS Equipment Due to a Natural Disaster. Protect the equipment as well as possible without moving it (time permitting) when a natural disaster occurs. DMDC will replace the equipment if damage occurs. If it is necessary to move the equipment and time permits, notify the APO. Note: Ensure RAPIDS equipment is included in the installation's disaster recovery plan. This requirement is explained in paragraph 4.5 of the RAPIDS Appendix S, Security Standard Operating Procedures (SSOP).
h. Workstation Deactivation/Reactivation guidelines. The RAPIDS workstation must always remain connected to the VPN.
(1) At the end of the day, the SSM must ensure users log off the workstation and reconnect to the VPN to enable the workstation to receive updates and downloads over non-work hours.
(2) If an update is not able to download overnight, the update will begin once the workstation reconnects to the VPN and can interrupt operations during the day.
(3) If a workstation remains disconnected from the VPN for over 30 days, it will be disabled and will not be able to be reactivated until a reactivation request is sent to the APO with the following requirements: 1) the availability of a network port for the workstation, 2) two certified SSMs at the site, and 3) a written action plan to maintain workstation compliance going forward.
(4) If the APO feels that the site has not made efforts to keep the workstation connected to the VPN and in compliance with all the required updates, the APO has the right to remove the workstation from the site. by DMDC.

1.13.2.2 Qualifications for the SSMs are as follows: The Contractor SSMs shall have at least two years of specialized experience performing CAC and USID Card functions and be capable of performing all duties and responsibilities of a Verifying Official (VO). SSMs shall have experience leading and supervising contract staff. SSMs shall have knowledge of, and ability to interpret, a variety of rules, regulations, procedures, and precedents relating to CAC and USID card functions. SSMs shall have the appropriate management and technical skills required to meet PWS requirements.

1.14 Identification of Contractor Personnel. All Contractor personnel attending meetings, occasionally answering government telephones, and working in other situations where their Contractor status is not

obvious to third parties, are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are government officials. They shall also ensure that all documents or reports produced by Contractors are suitably marked as Contractor products or that Contractor participation is appropriately disclosed.

1.14.1 All Contractor personnel performing work under this contract shall obtain a DoD CAC. The Contractor and any subcontractor(s) shall provide each employee an ID badge on the contract start date or on the employment start date. The ID badge shall, at a minimum, have the employee's name and the name of the Contractor or subcontractor. All Contractor/subcontractor personnel on duty shall wear identification badges on the upper front quadrant of the outer garment at all times when performing work under this contract. If wearing of the badge in the designated location should constitute a safety hazard, the Contractor shall designate an alternate location for display of the badge for the employee affected.

1.14.2 The Contractor shall develop, maintain, and provide to the COR an updated roster which shall include names and positions of all Contractor personnel as well as indicating which employees were issued CAC or other forms of government identification cards. The Contractor shall submit the initial roster to the COR within 10 calendar days after commencement of the contract's period of performance and every work day thereafter.

1.14.3 The Contractor shall immediately report any lost CAC or government-issued identification cards to the COR and Military and/or DoD police agencies. The Contractor shall immediately collect the CAC and other government-issued forms of identification upon termination of an employee, or at the end of the contract performance period. The CAC and other government-issued forms of identification shall be returned to the COR within one (1) hour of employee termination, or at the end of contract performance period, whichever comes first.

1.15 Contractor Personnel Appearance and Performance: It is essential that all Contractor personnel meet the highest standards of professionalism and personal integrity. The Contractor shall ensure personnel do not perform work under the influence of alcohol, illegal prescribed drugs or any other incapacitating agents. Contractor personnel shall be neatly groomed and dressed in business casual attire to present a professional appearance at all times.

1.16 Non-Conformance Report (NCR). When the Contractor's performance is unsatisfactory, an NCR will be issued. An NCR will be used whenever necessary in the administration of the contract to formally document nonconforming performance. The Contractor shall reply to the KO in writing within ten (10) work days from the date of receipt of the NCR, giving the reasons for the unsatisfactory performance, corrective action taken, and procedures to preclude recurrence.

1.17 The Contractor shall provide, to the COR/ACOR, corrective action plans, timely identification of issues, and effective management of subcontractors within ten (10) work days from the date of receipt of the NCR, or at a mutually agreed upon date.

1.18 Emergency Services. Emergency medical treatment services are available on Fort Bragg. In the event of an accident requiring emergency medical treatment, Contractor personnel can be transported to Fort Bragg facilities (Womack Army Medical Center). Once personnel are stabilized, they will be transported to a facility outside of Fort Bragg. The Contractor shall notify the KO or the COR/ACOR following any accident requiring emergency medical treatment, but not later than two (2) hours after the incident.

1.19 Data Rights. The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the Contractor without written permission from the KO. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

1.20 Organizational Conflict of Interest. Contractor and subcontractor personnel performing work under this contract may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the KO immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the KO to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of KO, and in the event the KO unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the KO may effect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

1.21 Transition (Phase-in/ Phase-out).

1.21.1 Phase-in.

1.21.1.1 During the Phase-in period, the Contractor shall prepare to assume full responsibility for all areas of operation in accordance with the terms and conditions of this contract. The Contractor shall have all personnel on board by the end of the thirty (30) calendar day Phase-in period. During the Phase-in period, the Contractor shall become familiar with performance requirements in order to commence full performance of services on the start of the base period of performance. The Contractor shall obtain their CAC or other form of government identifications, complete any specific government training, and conduct inventory and transfer of incidental GFP during the Phase-in period. The Contractor shall have Key Personnel identified in PWS paragraphs 1.13 and on-board during the entire Phase-in period.

1.21.2.2 Phase-Out

1.21.2.1 Prior to the completion of this contract, an observation period shall occur, at which time team management personnel of the incoming Contractor may observe operations. This will allow for orderly turnover of facilities, equipment, and records and will help to ensure continuity of services. The outgoing Contractor is ultimately responsible for performing full services in accordance with the contract, during the phase-out period, and shall not defer any requirements for the purpose of avoiding responsibility or of transferring, such responsibility to the succeeding Contractor. The outgoing Contractor shall fully cooperate with the succeeding Contractor and the Government, so as not to interfere with their work or duties.

1.21.2.2 To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the outgoing Contractor shall have all personnel on board during the phase-out period. The outgoing Contractor shall be prepared to transition the work load to the newly selected Contractor during the thirty (30) day phase-out period, which will occur at the end of the period of performance of the contractual effort.

1.21.2.3 Phase-out Plan. The Contractor shall develop a Phase-out Plan to affect a smooth and orderly transfer of contract responsibility to a successor. The Contractor shall provide the plan to the KO and COR thirty (30) days before the Phase-out period commences. The plan shall specify a training program and a date for transferring responsibilities for the work, and shall be subject to the KO's approval.

1.22. Addendum to FAR Clause 52.228-5 - Insurance Requirements: (reference *FAR 28.306, 28.307-2; 28.310; and FAR Clause 52.228-5.)* The following kinds and minimum amount of insurance coverage is required in accordance with Para (a) of FAR Clause 52.228-5 Insurance-Work on a Government Installation:

KIND	AMOUNT
Workers' Compensation	Amount required by the State in which this contract is performed; at least $100,000 except in States with exclusive or monopolistic funds that do not permit workers' compensation to be written by private carriers

Employer's Liability	$100,000 except in States with exclusive or monopolistic funds that do not permit workers' compensation to be written by private carriers
Comprehensive General Liability	$500,000 per occurrence for Bodily Injury
Comprehensive Automobile Liability	$200,000 per person $500,000 per occurrence for Bodily Injury $20,000 per occurrence for Property Damage

1.23. Limitations on Subcontracting (FAR Clause) 52.219-14: The Contractor shall submit evidence of compliance to the KO every six months starting from date of initial performance. Evidence may include a Contractor developed report that indicates the percentage of work performed by the prime contractor and the percentage of work performed by non-similarly situated entities. The report shall be supported by such facts as subcontractor billing and prime contractor payment.

1.24. Service Contract Reporting (SCR). (Applicable to a service contract with a total contract value exceeding $3M including all options. The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via Sam.gov. Reporting inputs shall be for the labor executed during the period of performance during each Government FY, which runs from October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported NLT October 31 of each calendar year. Contractors shall notify the KO and COR after the SCR is submitted.

1.24.1. Contractors shall enter the total dollar amount invoiced for services performed and the number of direct labor hours expended, to include first-tier subcontractor(s) under the contract, if applicable, during the previous Government FY. The direct labor hours expended are automatically converted into full time equivalent values. Note that under an indefinite delivery contract, reports are completed at the TO level and not at the contract level. The KO and COR will review the data for reasonableness and consistency. The KO will inform the Contractor if changes are necessary.

PART 2
DEFINITIONS & ACRONYMS

2. DEFINITIONS AND ACRONYMS:

2.1. Definitions:

2.1.1. CONFLICTING DIRECTIVES. Any apparent conflict between compliance with the directives, rules, and regulations identified in the contract and the satisfaction of the requirements of the contract shall be immediately brought to the attention of the KO for final resolution prior to performing the work involved. The Contractor shall notify the KO in writing in addition to any verbal notification of such conflict as soon as possible but NLT one (1) workday of the discovery of a conflict.

2.1.2. CONTRACTOR. A supplier or vendor awarded a contract to provide specific supplies or service to the Government. The term used in this contract refers to the prime.

2.1.3. CONTRACTING OFFICER (KO). Individual with the authority to enter, administer, and/or terminate contracts and make related determinations and findings. The term includes certain authorized representatives of the KO acting within the limits of their authority as delegated by the KO. The only individual who can legally bind the Government.

2.1.4. CONTRACTING OFFICER'S REPRESENTATIVE (COR). Individual designated and authorized in writing by the KO to perform specific technical or administrative functions. An employee of the U.S. Government appointed by the KO to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the Contractor, if that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.5. CONTRACTOR PERSONNEL. Includes Contractor and subcontractor employees performing working under this contract. Used interchangeably as Contractor employees.

2.1.6. *DAY. C*alendar day, unless otherwise specified.

2.1.7. DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the Performance Work Statement (PWS).

2.1.8. DELIVERABLE. Anything that can be physically delivered, but may include non-physical things, such as meeting minutes or reports.

2.1.9. FACILITY CLEARANCE. A facility clearance (FC) is an administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the same or lower classification category as the clearance being granted. The FC may be granted at the Confidential, Secret, or Top-Secret level. The FC includes the execution of DD441. Under the terms of the agreement, the Government agrees to issue the FC and inform the Contractor as to the security classification of information to which the Contractor will have access. The Contractor, in turn, agrees to abide by the security requirements set forth in the NISPOM (32 CFR Part 117).

2.1.10. GOVERNMENT-FURNISHED PROPERTY (GFP) OR GOVERNMENT PROPERTY (GP). Property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. Government-furnished property includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished

property also includes contractor-acquired property if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract.

2.1.11. INCIDENTAL PROPERTY. Property that is incidental to the place of performance, when the contract requires contractor personnel to be located on a government site or installation, and when the property used by the contractor within the location remains accountable to the Government. Items considered to be incidental to the place of performance include, for example, office space, desks, chairs, telephones, computers, and fax machines.

2.1.12. KEY PERSONNEL. Contractor personnel who are critical for achieving PWS objectives. Key personnel shall meet position qualification and experience requirements indicated in the PWS. When key personnel qualifications are used as an evaluation factor in "Best Value" procurement, the KO is the only one authorized to concur with key personnel replacement after award of the contract. When proposed key personnel resumes are used as an evaluation factor in best value procurement, a letter of commitment may be required from the individual whose resume is provided.

2.1.13. LOCAL TRAVEL. Any travel that is required to perform services IAW the PWS that is within a 50-mile radius of the place of performance.

2.1.14. OPERATIONS SECURITY (OPSEC). A security program involving primarily the protection of unclassified sensitive information from unauthorized disclosure.

2.1.15. PERFORMANCE WORK STATEMENT (PWS). A statement of work for performance-based acquisition that describes the required results in clear, specific, and object terms with measurable outcomes.

2.1.16. PERFORMANCE PREQUIREMENT SUMMARY (PRS). A listing of the service outputs under the contract that are to be evaluated by the COR on a regular basis, the surveillance methods to be used for these outputs, and the performance requirement of the listed outputs.

2.1.17. PHYSICAL SECURITY. Part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard against espionage, sabotage, damage, and theft.

2.1.18. PROPERTY ADMINISTRATOR (PA). The authorized representative of the KO appointed in accordance with agency procedures, responsible for administering the contract requirements and obligations relating to government property in the possession of a Contractor.

2.1.19. PROPERTY MANAGEMENT SYSTEM. The Contractor's system or systems for managing and controlling Government Property in its possession.

2.1.20. QUALITY ASSURANCE. A planned and systematic pattern of various functions, including inspections, performed by the Government necessary to provide confidence that adequate technical requirements are established; products and services conform to established technical requirements; and satisfactory performance is achieved.

2.1.21. QUALITY ASSURANCE SURVEILLAND PLAN (QASP). The Government's organized written document specifying the surveillance methodology to be used for surveillance of Contractor performance. The QASP is used for managing Contractor performance assessment by ensuring that systematic quality assurance methods validate that Contractor quality control efforts are timely, effective, and are delivering the results specified in the contract or task order. The QASP directly corresponds to the performance objectives and standards (i.e., quality, quantity, timeliness) specified in the Performance Work Statement (PWS). It provides specific details on how the Government will survey, observe, test, sample, evaluate, and document Contractor performance results to determine if the Contractor has met the required standards for each objective in the PWS. The QASP, with very few if any exceptions, is an internal to Government document.

2.1.22. QUALITY CONTROL. All necessary measures taken by the Contractor to assure that the quality of an end product or service shall meet contract requirements.

2.1.23. SHALL. An imperative command. Has a duty to or is required to. Denotes that a regulation or requirement must be followed.

2.1.24. SUBCONTRACTOR. Supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another
subcontractor. The Government does not have privity of contract with the subcontractor.

2.1.25. WORKDAY. The length of time during a day in which the Contractor provides services, in accordance with the contract. Also referred to as Business Day.

2.1.26. WORK WEEK. Monday through Friday, unless otherwise specified.

2.2. <u>ACRONYMS</u>:

ACOR	Alternate Contracting Officer's Representative
AD	Army Directive
AFARS	Army Federal Acquisition Regulation Supplement
AI	Army Instruction
AIE	Automated Installation Entry
AOR	Area of Responsibility
AR	Army Regulation
AT	Antiterrorism
ATCTS	Army Training Certification Tracking System
ATEP	Antiterrorism Enterprise Portal
CAC	Common Access Card
CAR	Corrective Action Request
CFR	Code of Federal Regulations
CHESS	Computer Hardware, Enterprise Software and Solutions
CICA	Competition in Contracting Act
CLIN	Contract Line-Item Number
CMDF	Controlled Material Destruction Facility
CONUS	Continental United States (excludes Alaska and Hawaii)
COR	Contracting Officer's Representative
COTS	Commercial Off the Shelf
CPARS	Contractor Performance Assessment Reporting System
CT	Compensatory Time
CTIP	Combating Trafficking in Persons
CUI	Controlled Unclassified Information
CY	Calendar Year (1 January – 31 December)
DA	Department of the Army
DD250	Department of Defense Form 250 (Receiving Report)
DD254	Department of Defense Form 254
DD1466	Building Pass
DES	Department of Emergency Services
DFARS	Defense Federal Acquisition Regulation Supplement
DMDC	Defense Manpower Data Center
DO	Delivery Order
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instructions
DoDM	Department of Defense Manual
DoDR	Department of Defense Regulation
DTM	Directive Type Memorandum

EN	Evaluation Notice
EO	Executive Order
ET	Eastern Time
FAR	Federal Acquisition Regulation
FFP	Firm Fixed Price
FFS	Full Food Service
FPCON	Force Protection Condition
FSO	Facility Security Officer
FSS	Federal Supply Schedule
FY	Fiscal Year (1 October – 30 September)
GAO	Government Accounting Office
GFE/M/P	Government Furnished Equipment/Material/Property
GPA	Government Property Administrator
HIPAA	Health Insurance Portability and Accountability Act of 1996
IA	Information Assurance
IAC	Installation Access Control
IACS	Installation Access Control System
IAW	In Accordance With
ICE	Interactive Customer Evaluation
IDIQ	Indefinite-Deliver Indefinite-Quantity
IGE	Independent Government Estimate
IRAPT	Invoicing, Receipt, Acceptance, and Property Transfer
IT	Information Technology
JPAS	Joint Personnel Adjudication System
JTR	Joint Travel Regulation
KO	Contracting Officer
KS	Contracting Specialist
LH	Labor Hours
LPTA	Lowest Price Technically Acceptable
MA	Multiple Award
MAS	Minimum Acceptable Standard
MATOC	Multiple Award Task Order Contract
MFR	Memorandum for Record
MICC	Mission and Installation Contracting Command
NACI	National Agency Check with Inquiries
NDA	Nondisclosure Agreement
NISP	National Industrial Security Program (32 CFR Part 2004)
NISPOM	National Industrial Security Program Operating Manual (32 CFR Part 117).
NLT	No Later Than
NTE	Not to Exceed
NTP	Notice to Proceed
OASIS	One Acquisition Solution for Integrated Services
OCI	Organizational Conflict of Interest
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Cost
OPSEC	Operations Security
OSHA	Occupational Safety and Health Act
OT	Over Time
PDREP	Product Data Reporting and Evaluation Program
PII	Personally Identifiable Information
PIPO	Phase-In/Phase- Out
PIT	Process Improvement Tracker
PM	Program Manager
PMSA	Property Management System Analysis
POC	Point of Contact
POP	Period of Performance

PRS	Performance Requirements Summary
PWS	Performance Work Statement
RA	Requiring Activity
RFI	Request for Information
RFP	Request for Proposal
RFQ	Request for Quotation
RTOP	Request for Task Order Proposal
QA	Quality Assurance
QAP	Quality Assurance Program
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Plan
SAM	System for Award Management
SB	Small Business
SCR	Service Contract Report
SME	Subject Matter Expert
SOP	Standard Operating Procedure
TARP	Threat Awareness and Reporting Program
TE	Technical Exhibit
TO	Task Order
TSDB	Terrorist Screening Database
U.S.C.	United States Code
VCC	Visitor Control Center
WAWF	Wide Area Workflow

PART 3
GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3. GOVERNMENT FURNISHED ITEMS AND SERVICES.

3.1 Facilities: The Government will provide Contractor PM with office space at in building 4-2843. The Government will provide workspaces for up to twenty (20) Contractor personnel at 4-2843 to provide support outlined in the PWS.

3.2. Utilities: The Government will provide the Contractor all utilities for their use in performing tasks outlined in this PWS. The Contractor shall instruct all employees in utilities conservation practices. The Contractor shall be responsible for operating under conditions that preclude the waste of utilities, which include turning off the water faucets, valves, light switches, etc., after using the required amount to accomplish the tasks requiring the use of utilities.

3.3 The Government will provide incidental property to the Contractor for use in performance of this contract. Such items include office space, desks, chairs, telephones, computers, ink pens, copier paper, DEERS RAPIDS Workstations, Multi-Function Devices, and fax machines.

3.3.1 The incidental property supplied to the Contractor meets the exception to FAR Part 45 as detailed in FAR 45.000(b)(5): "Government property that is incidental to the place of performance, when the contract requires contractor personnel to be located on a Government site or installation, and when the property used by the contractor within the location remains accountable to the Government."

PART 4
CONTRACTOR FURNISHED ITEMS AND SERVICES

4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES.

4.1 The Contractor shall furnish any supplies, equipment, facilities and services required to perform work under this contract that are not listed under Part 3 of this PWS.

PART 5

SPECIFIC TASKS

5. SPECIFIC TASKS. *All tasks listed in this part are deemed "Mission Essential Functions" and subject to DFARS Clause 252.237-7023, "Continuation of Essential Contractor Services."*

5.1. Basic Services and Staffing Requirements. The Contractor shall provide USID and CAC issuance support services in accordance with this PWS, regulations, publications, manuals, and local policies and procedures. The Contractor shall issue accurate and timely identification cards to all eligible recipients in accordance with AR 600-8-14.

5.1.1 The Contractor shall provide sufficient manpower to staff the following requirements during normal hours of operation and under emergency conditions.

5.1.1.1 14 RAPIDS Work Station contractors (08:00-12:00: 13:00-17:00) 8 hours a day.
5.1.1.2 Two (2) Customer Service Window contractors (08:00-12:00: 13:00-17:00) 8 hours a day.
5.1.1.3 Two (2) Telephone Appointment Line contractors (08:00-12:00: 13:00-17:00) 8 hours a day.
5.1.1.4 Two (2) Security Site Managers (SSMs) (08:00-12:00: 13:00-17:00) 8 hours a day.
5.1.1.5 For the above manpower requirements, a contracted duty position absence will be no longer than eight (8) consecutive operational hours of duty time. If an absence (illness, planned and unplanned leave, vacation, etc.) extends past eight (8) hours, the contractor will be replaced with a different fully qualified contractor.
5.1.1.6 Contractor will notify the COR and ACOR of planned and unplanned absences. Notification will be submitted by official email and telephonically. Notification will be within four hours of start of absence.

5.1.2 SSM Requirements.

5.1.2.1 The Contractor SSMs shall monitor all duties constantly (08:00-12:00: 13:00-17:00) to minimize customer waiting time.

5.1.2.2 SSMs shall install DMDC issued hardware and software components, run and review audit reports, manage users, security, cardstock, consumables, and maintain the site's address information/hours of operations/business practices (appointment only or walk-ins) for the "ID Card Office Online," Security Online, and Inventory Logistics Portal (ILP). The SSM shall also perform RAPIDS security overrides for document and fingerprint support. The SSMs shall perform the following tasks:

A. Prepare correspondence, letters, and, statistical reports as required by the ID Card Facility Manager or COR;
B. Enter and/or validate data in automated systems, as needed;
C. Maintains accuracy of automated personnel and other databases;
D. Retrieve data from the Rapids Reporting Tool, DHR databases, and site maintenance tool;
E. Review and verify records to identify discrepancies and gaps in information;
F. Interview personnel to obtain additional information as needed to complete record and/or to correct discrepancies;
G. Maintain required forms, records, and files pertaining ID Card procedures;
H. Enter and/or validate data in automated systems, as needed;
I. Maintain "ID Card Office Online" oversight;
J. Review all information on the audit trail reports;
K. Evaluate the audit trail report to monitor for fraud, waste, and abuse, and maintain for one year and/or during the period of performance;
L. Accompany the Government SSM on unit site visits to assist in the operation of their deployable RAPIDS Workstations.

5.1.2.3 All SSMs shall complete the VOs training and Send RAPIDS Verifying Officials (VO) Desktop

Certification, and Send RAPIDS Verifying Officials (VO) Deployable Certification. Certificates of training completion shall be submitted to the KO and COR prior to the employee performing work under the contract.

5.1.3 Verifying Officials (VOs)

5.1.3.1 All Contractor personnel staffing RAPIDS Workstations, Customer Service Windows, Telephone Appointment Lines, and Telephone Customer Service Lines shall be certified as "VOs."

5.1.3.2 All VOs shall complete the following training: RAPIDS Verifying Officials (VO) Desktop Certification, and RAPIDS Verifying Officials (VO) Deployable Certification. Certificates of training completion shall be submitted to the KO and COR prior to the employee performing work under the contract.

5.2. Issuance of Cards.

5.2.1 CAC.

5.2.1.1 The Contractor shall be responsible for accountability, control, verification and issuance of military CAC and the reset of CAC Personal Identification Numbers (PIN) for active duty military, Reserve and National Guard members, and other eligible recipients. For every customer receiving a new CAC, the Contractor shall generate and obtain signature on a DD Form 2842, DoD Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities. At least 85% of CAC issuance shall be completed in no more than 20 minutes and CAC PIN Resets shall be within 15 minutes from the time the customer sits down at the VO's desk until they leave with their CAC. The COR will monitor compliance through direct observation periodically.

5.2.1.2 The Contractor shall perform all tasks relating to CAC issuance, to include researching and reviewing source documents, verifying eligibility, and discussing entitlements as defined in Air Force Instruction (AFI) 36- 3026 IP Volume 1, Certification Practice Statement (CPS), and the RAPIDS Training Guide. The CPS and RAPIDS Training Guide will be made available to the Contractor after award.

5.2.2 USID Cards.

5.2.2.1 The Contractor shall be responsible for accountability, control, verification and issuance of USID cards to military retirees, family members/dependents, and other eligible recipients. At least 85% of USID cards shall be completed in no more than 30 to 45 minutes from the time the customer sits down at the VO's desk until they leave with their ID Card. The COR will monitor compliance through direct observation periodically.

5.2.2.2 The Contractor shall perform all tasks relating to ID card issuance, to include researching and reviewing source documents, verifying eligibility, and discussing entitlements as defined in AFI 36- 3026 IP, CPS, and the RAPIDS Training Guide.

5.2.2.3 The Contractor shall complete at least 85% of DEERS inputs/updates no more than 30 minutes from the time the customer sits down at the VO's desk until their record is updated. The COR will monitor compliance through direct observation periodically.

5.2.4 Shop for Cards.

5.2.4.1 The SSC Facility is designated as the personal agent to authorize a specific, named person to shop for or assist an authorized patron at the Fort Bragg commissary or exchange. The SSC Facility issues a durable plastic Shop for Card in lieu of an authorization letter. The Contractor shall issue Shop for Cards in accordance with the local policy and Air Force Instruction (AFI) 36-3026 IP Volume 1.

5.3 DEERS RAPIDS Inputs.

5.3.1 The Contractor shall register, process, and maintain customers' DEERS RAPIDS information. The Contractor shall identify the appropriate privileges for each recipient. The Contractor shall ensure inputs and updates are accurate and in compliance with AFI 36-3026 IP Volume 1.

5.3.2 The Contractor shall complete at least 85% of DEERS inputs/updates no more than 30 minutes from the time the customer sits down at the VO's desk until their record is updated. The COR will monitor compliance through direct observation periodically.

5.4 Appointment Scheduling.

5.4.1 The "ID Card Office Online" Web-Based Scheduling. The Contractor shall maintain oversight of the "ID Card Office Online" website via the Site Maintenance Tool, to include monitoring online appointments, ensuring the website is operational, opening/closing appointments, and updating information as needed.

5.4.2 Telephonic Scheduling. The Contractor shall take appointments via telephone scheduling lines (910-396-9339/2737). The Contractor shall ensure all appointments are entered in the "ID Card Office Online" web-based scheduling system before the close of business day.

5.4.2.1 The Contractor shall take incoming calls, answer questions, and direct callers to the proper agencies at the SSC as needed. The appointment lines shall be manned by a certified VO.

5.5 Customer Service Window Operations.

5.5.1 The Contractor shall screen customers in at least two of the four SSC customer service windows during check-in and enter required information and requested action for eligible recipients into a Government database/kiosk. The Contractor shall ensure customers have all necessary information before entering customers into the database/kiosk. The Customer service windows shall be manned by a certified VO.

5.5.2 The SSMs shall monitor kiosks constantly to minimize customer waiting time. Contractor VOs shall monitor and retrieve customers out of the kiosk customer log, and when service is complete on that customer, the VO shall sign the customer out of the kiosk and immediately pull the next available customer.

5.6 Reports.

5.6.1 The Contractor shall prepare Monthly Status Reports (MSRs) and submit to the COR not later than the 5th working day of every month. The MSRs shall describe activities of those assigned to the project, problems encountered, actual or recommended corrective action. In addition, the report shall include monthly workload performed and quality control results. At a minimum, the Contractor shall address workload items included in TE 1 - "Historical Workload Data," TE 2 - "Performance Requirements Summary (PRS)," and address whether or not standards described in the PRS are being met.

5.6.2 Damages Caused by Contractor. Damages to Government equipment caused by Contractor employees shall be reported to the COR/ACOR and KO upon occurrence.

5.6.3 The Contractor shall prepare, revise, and print correspondence in the proper format under applicable regulations and guidelines IAW AR 25-50.

5.7 Additional Requirements.

5.7.1 The Contractor shall request work orders related to internet and phone system issues (such as logging on, software updates, etc.) from the Army Enterprise Service Desk and Directorate of Human Resources Information Technology section as needed.

5.7.2 The Contractor shall perform routine maintenance on computers and printers (i.e. change ribbons, add toner and developer, clean printers) for each of the 17 work stations manned by Contractor personnel. This routine maintenance shall be performed in accordance with the RAPIDS 7, User Guide, and Version 2.9, dated October 2019.

5.7.3 The Contractor shall accomplish tasks to manage internal and external databases associated with activities created and analyzing to continuously improve efficiency, effectiveness, and quality. The Contractor shall compile data on performance, prepare recurring and special reports, and respond to a variety of internal and external customer requests to include order creation, status, and general information. The Contractor shall review, verify, and provide feedback to stakeholders and leadership.

PART 6
APPLICABLE PUBLICATIONS

6. APPLICABLE PUBLICATIONS. The Contractor shall abide by all applicable regulations, publications, manuals, and local policies and procedures. When a publication provided by the Government is subsequently revised, supplemented, replaced or rescinded, the Contractor, upon notification or receipt, shall comply. The following websites can be used to find publications and regulations:

https://armypubs.army.mil/
https://www.e-publishing.af.mil/
https://www.esd.whs.mil/Directives/issuances/dodm/

6.1 AR 25-50, "Preparing and Managing Correspondence" (10OCT2020)

6.2 AR 385-10, "The Army Safety and Occupational Health Program" (24JUL2023)

6.3 DoD Instruction 1000.13, ID Cards for Members of the Uniformed Services, their Dependents, and Other Eligible Individuals (rev 23JAN2014)

6.4 DoD Manual 1000.13, Volume 1, DoD ID Cards: ID Card Lifecycle (rev 23JAN2014)

6.5 DoD Manual 1000.13, Volume 2, DoD ID Cards: Benefits for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals (rev 23JAN2014)

6.6 DoD Instruction 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC) (09SEP2014) with Change 2, effective (2NOV 2020)

6.7 DoD Instruction 1341.02, Defense Enrollment Eligibility Reporting Systems (DEERS) Program and Procedures (18AUG2016)

6.8 Federal Information Processing Standards (FIPS) Publication 201-3 (published JAN2022)

6.9 Appendix S Security Standard Operating Procedures (SOP) for Real-time Automated Personnel Identification System (RAPIDS) Version 7xx Workstation/Laptop System, 24 Aug 2010

6.10 RAPIDS User Guide Compiled v1.0 (Feb2025)

PART 7
TECHNICAL EXHIBIT (TE) LISTING

TE 1 – Performance Requirements Summary (PRS) Matrix

TE 2 – Deliverables Schedule

TE 3 – Historical Workload Data

Technical Exhibit 1

PERFORMANCE REQUIREMENTS SUMMARY (PRS) MATRIX

Required Services	Performance Standard	Acceptable Quality Level (AQL)	Incentive (Positive and/or Negative)
PWS 5.2. Accurate and timely issuance of CACs to eligible recipients.	The Contractor shall issue CACs IAW AFI 36-3026 IP Volume 1, and at least 85% of CACs issued within 20 minutes.	Quality: 100% Accuracy; Timeliness: 85% issued within 20 minutes	Contractor compliance rate shall be utilized as objective evidence of contract compliance and documented into the CPAR System
PWS 5.2.2. Accurate and timely issuance of USID cards to eligible recipients	The Contractor shall issue USIDs IAW AFI 36-3026 IP Volume 1, and at least 85% of USIDs issued within 15 minutes	Quality: 100% Accuracy; Timeliness: 85% issued within 15 minutes	Contractor compliance rate shall be utilized as objective evidence of contract compliance and documented into the CPAR System
PWS 5.3. Timely updates to records in the DEERS/ RAPIDS system.	The Contractor shall complete at least 85% of inputs/updates and Pin Resets within 15 minutes	Quality: 100% Accuracy; Timeliness: 85% updated within 15 minutes	Contractor compliance rate shall be utilized as objective evidence of contract compliance and documented into the CPAR System
PWS 5.1 Accurate records of all appointments posted to calendar daily before the close of business.	The Contractor shall accurately record all appointments in calendar daily before the close of business.	Quality: 100% accuracy Timeliness: Record before end of business day	Contractor compliance rate shall be utilized as objective evidence of contract compliance and documented into the CPAR System

Technical Exhibit 2

DELIVERABLES

Deliverable	Frequency	# Of Copies	Medium/Format	Submit To
01 Quality Control Plan (PWS para. 1.6.1)	Once initially, updates submitted as occur	2	MS Word	KO/Contract Specialist & COR/ACOR
02 Physical Security Checklist or Log (PWS para. 1.7.6.1.5)	Monthly	2	Army Standard Form (SF) 701 Activity Security Checklist	KO/Contract Specialist & COR/ACOR
03 Training Completion Certificates (PWS paras. 5.1.2.3; 5.1.3.2)	Once initially, and annually thereafter	2	Electronic	KO/Contract Specialist & COR/ACOR
04 Mission-Essential Contractor Services Plan Updates (PWS para. 1.10)	As occurs	2	MS Word	KO/Contract Specialist & COR/ACOR
05 Post Award Meeting (PWS para. 1.11)	Periodic	N/A	Meeting/Briefing	KO/Contract Specialist & COR/ACOR
06 Name of PM (PWS para. 1.13.1)	As hired	2	MS Word	KO/Contract Specialist & COR/ACOR
07 Personnel Roster PWS para. 1.14.2	Daily	1	Electronic	COR
08 Response to NCRs (PWS para. 1.17)	As occurs	2	PDF with digital signature	KO/Contract Specialist & COR/ACOR
09 Notification of Accident Requiring Emergency Services (PWS para. 1.18)	As occurs	2	Electronic	KO/Contract Specialist & COR/ACOR
10 OCI Notifications and Mitigation Plan (PWS para. 1.20)	As occurs	1	MS Word	KO
11 Phase-out Plan (PWS para. 1.21.2.3)	Once	2	MS Word	KO/Contract Specialist & COR/ACOR
12 Monthly Status Report (PWS para. 5.6.1)	Monthly	2	MS Word	KO/Contract Specialist & COR/ACOR

Technical Exhibit 3

HISTORICAL WORKLOAD DATA

1. Estimated Annual Workload Data CY21 that does not include December 2021

Item Description	Annual Workload
Extended Hours of Operation (IAW PWS para 1.6.4.1 Extended hours of Operations)	0
CAC cards issued	46,366
CAC PIN resets	5,401
USIDs issued	27,264
DEERS Enrollments processed	59,575
Appointments made by phone	34,984
Customers assisted at service windows	44,047

2. Estimated Annual Workload Data CY 22 that does not include December 2022

Item Description	Annual Workload
Extended Hours of Operation (IAW PWS para 1.6.4.1 Extended hours of Operations)	0
CAC cards issued	52,709
CAC PIN resets	4,647
USIDs issued	33,799
DEERS Enrollments processed	61,535
Appointments made by phone	38,551
Customers assisted at service windows	50,766

3. Estimated Annual Workload Data CY23 that does not include December 2023

Item Description	Annual Workload
Extended Hours of Operation (IAW PWS para 1.6.4.1 Extended hours of Operations)	0
CAC cards issued	41,355
CAC PIN resets	3,750
USIDs issued	27,962
DEERS Enrollments processed	4,639
Appointments made by phone	34,483
Customers assisted at service windows	50,664

4. Estimated Annual Workload Data CY24 that does not include December 2024

Item Description	Annual Workload
Extended Hours of Operation (IAW PWS para 1.6.4.1 Extended hours of Operations)	0
CAC cards issued	50,908
CAC PIN resets	4,763
USIDs issued	29,750
DEERS Enrollments processed	7,048
Appointments made by phone	25,026
Customers assisted at service windows	56,523

5. Estimated Annual Workload Data CY25 that does not include December 2025

Item Description	Annual Workload
Extended Hours of Operation (IAW PWS para 1.6.4.1 Extended hours of Operations)	0
CAC cards issued	44,920
CAC PIN resets	4,864
USIDs issued	22,518
DEERS Enrollments processed	7,099
Appointments made by phone	19,033
Customers assisted at service windows	42,703

6. Historic Work Load Labor Categories

Labor Category	FT/PT	Excempt/non-excempt	Location	Wage Code	No. Emp.	Net PROD Hours
Program Manager	FT.	Exempt	N/A	Exempt	1.0	1920
Site Security Manager	FT	Non- Exempt	Fort Bragg NC	Personnel Assistant (Employment) III	2.00	3840
Verifying Officials	FT	Non- Exempt	Fort Bragg NC	Personnel Assistant (Employment) II	18.00	34560

NOTE: The extended hours of operation utilized three contractor employees for one-hour each occasion