PERFORMANCE WORK STATEMENT (PWS)

FOR

Central Issuing Facility (CIF) Support Services

1.0 General:

1.1 Scope: The contractor shall provide all personnel, equipment, tools, materials, supervision, and quality control necessary, except as specified in Paragraph 3.0 as Government Furnished, to perform Central Issuing Facility (CIF) Support Services, as defined in this PWS.

1.2 Background: The Pennsylvania Army National Guard requires contractor support to sustain Central Issuing Facility (CIF) operations at Fort Indiantown Gap. The state requires two contractor personnel to support issue, exchange, turn-in, records, warehouse, and customer service functions associated with Organizational Clothing and Individual Equipment (OCIE). This requirement is intended to improve customer throughput, maintain accountability documentation, support readiness, and reduce delays in CIF operations.

1.3 Period of Performance (PoP): The PoP shall be one year of 12 months from 15 June 2026 to 14 June 2027.

1.4 General Information:

1.4.1 Place and Performance of Services: The contractor shall provide services between the hours of 0700-1630 on Monday through Friday except on recognized US holidays or when the Government facility/installation is closed due to local or national emergencies, administrative closings, or similar Government-directed facility/installation closings. Performance shall be at Central Issuing Facility (CIF), BLDG 14-12, Fort Indiantown Gap (FTIG), Annville, PA. The contractor shall, at all times, maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility/installation 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.

1.4.1.1 Telework: Telework is not authorized under this requirement. The required services involve in-person customer interface, physical receipt, issue, inspection, handling, storage, and movement of OCIE and related CIF stock.

1.4.1.2 Unscheduled gate closures by the Security Police may occur at any time causing all personnel entering or exiting a closed installation to experience a delay. This cannot be predicted or prevented. Contractors are not compensated for unexpected closures or delays. Vehicles operated by contractor personnel are subject to search pursuant to applicable regulations. Any moving violation of any applicable motor vehicle

regulation may result in the termination of the contractor employee's installation driving privileges.

1.4.1.3 The contractor's employees shall become familiar with and obey the regulations of the installation, including fire, traffic, safety, and security regulations while on the installation. Contractor employees should only enter restricted areas when required to do so and only upon prior approval. All contractor employees shall carry proper identification with them at all times and shall be subject to such checks as may be deemed necessary. The contractor shall ensure compliance with all regulations and orders of the installation, which may affect performance. The Government reserves the right to direct the removal of an employee from Government property or revoke access to Government systems for misconduct, security reasons, or any overt evidence of communicable disease. Removal of contractor employees for reasons stated above does not relieve the Contractor from responsibility for total performance of this contract.

1.4.2 Recognized Holidays: The following are recognized US holidays. The contractor shall not perform services on these days:

1.4.2.1 New Year's Day: January 1st
1.4.2.2 Martin Luther King, Jr.'s Birthday
1.4.2.3 President's Day
1.4.2.4 Memorial Day
1.4.2.5 Juneteenth: June 19th
1.4.2.6 Independence Day: July 4th
1.4.2.7 Labor Day
1.4.2.8 Columbus Day
1.4.2.9 Veteran's Day: November 11th
1.4.2.10 Thanksgiving Day
1.4.2.11 Christmas Day

1.4.3 Quality Control (QC): The contractor shall develop and maintain an effective QC Plan (QCP) to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor's QCP is the means by which it assures itself that its work complies with the requirements of the contract. As a minimum, the contractor shall develop QC procedures that address the areas identified in Technical Exhibit 1, Performance Requirements Summary. After acceptance of the QCP, the contractor shall obtain the KO acceptance in writing of any proposed changes to its QCP.

1.4.4 Quality Assurance (QA): The Government shall 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 Government must do to ensure that the contractor has performed in accordance with the performance standards. It

defines how the performance standards will be applied, the frequency of surveillance, and acceptable quality level(s) or defect rate(s).

1.4.5 Installation Access and Security Requirements. The contractor shall comply with all applicable installation/facility access and local security policies and procedures, which may be obtained from the COR. The contractor and all associated subcontractor employees shall provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services, or Security Office. The contractor shall ensure compliance with all personal identity verification requirements as directed by Department of Defense (DoD), Headquarters Department of Army (HQDA) and/or local policy (see PWS 6.0). Should the Force Protection Condition (FPCON) change, the Government may require changes in contractor security matters or processes.

1.4.5.1 For contractors requiring Common Access Card (CAC): The CAC is the DoD Federal Personal Identity Verification (PIV) credential. Before CAC issuance, the contractor employee requires, at a minimum, a favorably adjudicated Tier 1, or an equivalent or higher, investigation in accordance with Army Directive 2014-05. The contractor employee will be issued a CAC only if duties involve one of the following: (1) both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) physical access to multiple DoD facilities or multiple non DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of 6 months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully scheduled Tier 1 investigation at the Office of Personnel Management.

Sponsorship and enrollment information about each applicant must be registered in the Defense Enrollment Eligibility Reporting System (DEERS) through either the Real-Time Automated Personnel ID System (RAPIDS) using the DD Form 1172-2 or the Trusted Associate Sponsorship System (TASS).

1.4.5.1.1 Homeland Security Presidential Directive (HSPD)-12 Background Investigation Requirements: The contractor shall ensure that all contractor and subcontractor personnel whose duties require CAC card issuance obtain them and shall process all CAC card applications. The contractor shall ensure that all employees requiring an initial background investigation complete a Personnel Security Investigation Portal (PSIP) completed at the earliest possible date and that this form is forwarded to the COR 15 days of hire. The COR will review the form for completeness and accuracy and forward it to the National Guard Bureau (NGB) Personnel Security manager who will initiate the investigation process via the PSIP. Contractor personnel will then receive two e-mail messages; the first will confirm that the investigative service provider has received the request, and the second will provide instructions for the completion of the appropriate form via the Electronic Questionnaires for Investigations Processing (e-QIP) system. Upon completion of the e-QIP questionnaire and submission of all required documents, including fingerprint card to the security manager, the background investigation (BI) will be initiated. The contractor shall ensure

immediate compliance with all instructions regarding background investigation processing, including those provided verbally, by e-mail, or via a Government system. The contractor is cautioned that the entire process from submittal of the PSIP form to return of the FBI fingerprint check may routinely take from two to six weeks and shall factor this lead time into its hiring/placement process. The contractor shall make all reasonable efforts to ensure that contractor employees meet CAC eligibility standards upon assignment to the contract and shall be held responsible for delays, failure to meet performance requirements, or decreases in efficiency in accordance with the applicable inspection clause.

Sponsorship and enrollment information about each applicant must be registered in the Defense Enrollment Eligibility Reporting System (DEERS) through either the Real-Time Automated Personnel ID System (RAPIDS) using the DD Form 1172-2 or the Trusted Associate Sponsorship System (TASS).

1.4.5.1.2 Trusted Associate Sponsorship System TASS: The contractor shall process CAC applications through the TASS, the procedures for which are described below. Although there is no requirement for the contractor to designate a “Corporate Facility Security Officer" (FSO) to serve as its single point of contact for the BI, the TASS application process and other CAC and security-related matters, such designation facilitates these processes. If a Corporate FSO is not established, all contractor employees requiring a CAC will be required to process their own applications. The submission process for CAC applications is as follows:

1. The contractor's FSO or contractor employee shall submit requests for a CAC via email to the designated TASS Trusted Agent (TA) before accessing the TASS website. The TASS TA for this requirement will be: Major Wendy Mroz.

2. The Government will establish a TASS application account for each CAC Request and will provide each contractor employee a USER ID and Password, via email, to the FSO. The FSO or contractor employee shall access the TASS account and complete the CAC application (entering/editing contractor information as applicable) at: https://www.dmdc.osd.mil/tass/ . The contractor’s FSO or contractor employee will submit completed applications in TASS and will follow up to ensure that the TA is processing the request.

3. The Government will inform the contractor's applicant, via email, of one of the following:

   a. Approved.* Upon approval, the information is transferred to the Defense Enrollment Eligibility Reporting System (DEERS) database and an email notification is sent to the contractor with instructions on obtaining their CAC. The contractor proceeds to a Real-Time Automated Personnel Identification System (RAPIDS) station (RAPIDS Site Locator: http://www.dmdc.osd.mil/rsl/).

   b. Rejected.* The Government, in separate correspondence, will provide reason(s) for rejection.

c. Returned. Additional information or correction to the application required by the contractor employee.

*The contractor shall maintain records of all approved and rejected applications.

1.4.5.1.3 At the RAPIDS station, the RAPIDS Verification Officer will verify the contractor employee by Social Security Number (SSN) and two forms of identification. Identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1615-0047, "Employment Eligibility Verification". Consistent with applicable law, at least one document from the Form I-9 list shall be a valid (unexpired) State or Federal Government-issued picture ID. The Identity documents will be inspected for authenticity and scanned and stored in the DEERS upon issuance of an ID. The photo ID requirement cannot be waived, consistent with applicable statutory requirements. The Verification Officer will capture primary and alternate fingerprints, picture, and updates to DEERS, and will then issue a CAC. Issued CACs will be valid for no longer than three years, or until the individual's contract end date (inclusive of any options), whichever is earlier.

1.4.5.1.4 The contractor shall manage requests for new or renewal CAC cards in sufficient time to ensure that all contractor employees have them when needed to perform work under this contract. The contractor shall provide at least 10 calendar days advance notice to the TA, unless there are extenuating circumstances approved by the COR or KO.

1.4.5.1.5 The contractor shall return issued CACs to the DEERS office upon departure or dismissal of each contractor employee, and shall obtain a receipt for each card and provide it to the TA/COR.

1.4.5.1.5.1 Failure to comply with these requirements may result in withholding of final payment.

1.4.5.1.6 The contractor shall obtain a military/federal email address for each applicant, including subcontractors, who may be deployed or require logical access to a Government computer network. Note: If employees of a contractor lose the privilege to access these systems, they lose the ability to renew their CAC. Therefore, it is critical that contractor employees maintain their accounts.

1.4.5.2 For contractors that do not require a CAC, but require access to a DoD facility or installation: Contractor and all associated sub-contractors employees shall comply with adjudication standards and procedures in PMR 525- 2 Annex C Appendix 2 Para 1-4, and applicable installation, facility and area commander installation/facility access, and local security policies and procedures (provided by a Government representative).

1.4.5.3 Awareness Training (AT) Level 1: All contractor employees, including

subcontractor employees, requiring access to Army installations, facilities, and controlled access areas shall complete AT Level 1 training within 30 calendar days after contract start date and within 30 calendar days of new employees commencing performance. The contractor shall submit certificates of completion for each affected contractor and subcontractor employee to the COR within 15 calendar days after completion of training by each employee or subcontractor personnel. AT Level 1 awareness training is available at the following website: https://jko.jten.mil/courses/AT-level1/launch.html .

1.4.5.4 iWATCH Training: The contractor and all associated subcontractors with an area of performance within an Army-controlled installation, facilities or area shall brief all employees on the local iWATCH program (training standards provided by the requiring activity Antiterrorism Officer (ATO)). This local developed training shall be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR or the KO. This training shall be completed within 30 calendar days of contract award and within 30 calendar days of new employees commencing performance. The contractor shall report completion for each contractor employee and subcontractor employee to the COR within 15 calendar days after completion of training.

1.4.5.5 Communications Security/Information Technology (COMSEC/IT) Security. All communications with DoD organizations are subject to COMSEC review. All telephone communications networks are continually subject to intercept by unfriendly intelligence organizations. DoD has authorized the military departments to conduct COMSEC monitoring and recording of telephone calls originating from, or terminating at, DoD organizations. Therefore, the contractor is advised that any time contractor personnel place or receive a call they are subject to COMSEC procedures. The contractor shall ensure wide and frequent dissemination of the above information to all employees dealing with DoD information. The contractor shall abide by all Government regulations concerning the authorized use of the Government's computer network, including the restriction against using the network to recruit Government personnel or advertise job openings.

1.4.5.6 Use of Government Information Systems (IS) and access to Government networks is a revocable privilege, not a right. Users are the foundation of the DoD strategy, and their actions affect the most vulnerable portion of the Army Enterprise Infostructure (AEI). Contractor employees shall have a favorable background investigation or hold a security clearance and access approvals commensurate with the level of information processed or available on the system. Contractor employees shall:

1.4.5.6.1 Comply with the command's Acceptable Use Policy (AUP) for Government owned IS and sign an AUP prior to or upon account activation.

1.4.5.6.2 Complete initial and/or annual Information Assurance (IA) training as defined in the IA Best Business Practices (BBP) training_

(https://atc.us.army.mil/iastar/docs/Training_BBP.pdf).

1.4.5.6.3 Mark and safeguard files, output products, and storage media per classification level and disseminate them only to individuals authorized to receive them with a valid need to know.

1.4.5.6.4 Protect IS and IS peripherals located in their respective areas in accordance with physical security and data protection requirements.

1.4.5.6.5 Practice safe network and Internet operating principles and take no actions that threaten the integrity of the system or network.

1.4.5.7 Army Training Certification Tracking System (ATCTS): All contractor employees with access to a Government information system shall be registered in ATCTS (https://atc.us.army.mil/iastar/index.php) at commencement of services, and shall successfully complete the DoD Information Assurance awareness training prior to access to the IS and then annually thereafter. (https://iatraining.us.army.mil/).

1.4.5.8 IA Training. All contractor employees and associated subcontractor employees shall complete the DoD IA Awareness Training before issuance of network access and annually thereafter.

1.4.5.9 IA/Information Technology (IT) certification. All contractor employees performing services involving IA/IT functions shall comply with DoD and Army workforce training requirements in DoDD 8140.01, DoD 8570.01-M and AR 25-2 within six months of the start of contract performance or appointment to IA/IT functions. In accordance with DoD8570.01-M, DFARS 252.239.7001, and AR 25-2, contractor employees supporting or performing IA/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M shall be completed upon contract award.

1.4.5.10 Protection of Personally Identifiable Information (PII). The contractor shall protect all PII encountered in the performance of services in accordance with Defense Federal Acquisition Regulation Supplement (DFARS) 224.103 Personally Identifiable Information and Department of Defense Directive (DoDD) 5400.11, Department of Defense Privacy Program, and DoD 5400.11-R. If a PII breach results from the contractor's violation of the aforementioned policies, the contractor shall bear all notification costs, call-center support costs, and credit monitoring service costs for all individuals whose PII has been compromised.

1.4.5.11 OPSEC Training: In accordance with AR 530-1, Operations Security, new contractor employees shall complete Level I OPSEC training within 30 calendar days of their reporting for duty and annually thereafter. The contractor shall submit certificates of completion for each contractor employee to the COR (if no COR is assigned, delete to the COR and replace with to the KO) within 15 calendar days after completion of training. Level 1 OPSEC training is available at

https://securityawareness.usalearning.gov/opsec/index.htm.

1.4.5.12 OPSEC SOP/Plan The contractor shall develop an OPSEC Standard Operating Procedure (SOP)/Plan and provide it to the COR within 90 calendar days of contract award to be reviewed and approved by the responsible Government OPSEC officer, per AR 530-1, Operations Security. This SOP/Plan shall include a process to identify the Government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. The contractor shall implement OPSEC measures as required by the Government. In addition, the contractor shall identify an individual who will be an OPSEC Coordinator. The contractor shall ensure this individual becomes OPSEC Level II certified within 90 days of appointment as OPSEC coordinator in accordance with AR 530-1. Contractor shall provide a copy of the certification to the COR NLT 15 days after completion.

1.4.5.13 Classified Information. This contract does not require handling of or access to classified information.

1.4.5.14 Threat Awareness and Reporting Program (TARP). Per AR 381-12, Threat Awareness and Reporting Program (TARP), contractor employees with security clearances must receive annual TARP training by a counterintelligence (CI) agent or other trainer as specified in Chapter 2 Threat Awareness and Education, Section II, paragraph 2-4b. The contractor shall identify annual TARP training, personnel trained, and date of training within 15 days of training completion.

1.4.6 Physical Security. The contractor shall safeguard all Government property provided for contractor use. At the close of each work period, Government facilities, equipment, and materials shall be secured.

1.4.6.1 Key Control: NOTE: All references to keys include key cards. The contractor shall establish and implement methods of ensuring that no keys/key cards issued by the Government are lost or misplaced or are used by unauthorized persons. No keys issued by the Government shall be duplicated**.** Such procedures shall include turn- in of any issued keys by personnel who no longer require access to locked areas. The contractor shall include procedures covering key control in the QCP.

1.4.6.1.1 The contractor shall immediately report any occurrences of lost or duplicated keys/key cards to the COR.

1.4.6.1.2 In the event keys, other than master keys, are lost or duplicated, the contractor shall, upon direction by 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 Government replaces or re-keys the locks, the Government will deduct the total cost of lock replacement or re-keying from the monthly payment due the contractor. In the event a master key is lost or duplicated, the Government will replace all locks and keys for that system, and will deduct the total cost

from the monthly payment due the contractor.

1.4.6.1.3 The contactor shall prohibit the use of the 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 contactor employees engaged in the performance of services in those areas, or personnel authorized entrance by the KO.

1.4.6.2 Lock Combinations: The contractor shall establish and implement methods of ensuring that no lock combinations are 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.

1.4.7 Special Qualifications: CIF support specialists shall, within 60 days of appointment, complete all required local CIF, installation, warehouse, safety, and system familiarization training necessary to perform this requirement. Contractor personnel shall comply with any new training requirements resulting from changes in regulation, local policy, or mission need at no additional cost to the Government.

1.4.8 Post Award Conference/Periodic Progress Meetings: The contractor agrees to attend any post award conference convened by the KO in accordance with Federal Acquisition Regulations Subpart 42.5. The KO, COR, and other Government personnel, as appropriate, may meet periodically with the contractor to review the contactor's performance. At these meetings, the Contacting Officer will apprise the contractor of how the Government views the contractor's performance and the contractor shall apprise the Government of problems, if any, being experienced. The contractor shall resolve outstanding issues raised by the Government. Contractor attendance at these meetings shall be at no additional cost to the Government. Periodic progress meeting are to be scheduled on a biannual basis.

1.4.9 Contract Manager (CM): The contactor shall designate a CM who shall ensure performance under this contract. The name of this person, and an alternate who shall act for the contractor when the CM is absent, shall be designated in writing to the KO. The CM or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract. The CM shall work through the COR, (or the KO if a COR is not assigned), to resolve issues, receive technical instructions, and ensure adequate performance of services. The CM shall ensure that contractor employees do not perform any services outside the scope of the contract without an official modification issued by the KO. The CM shall ensure contractor employees understand that services performed outside the scope of the contract are performed wholly at the expense of the contractor.

1.4.10 Identification of Contractor Employees: All contractor personnel attending meetings, 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 that they are Government employees.

The contractor shall ensure that all documents or reports produced by contractor personnel are suitably marked as contractor products or that contractor participation is appropriately disclosed. The contractor's status as a "contractor" shall be predominantly displayed in all correspondence types (to include signature blocks on e-mail) and dealings with Government or non-Government entities/ Contractor personnel shall wear identification badges distinguishing themselves as such. The badges shall have the company name, employee name and the word "contractor" displayed.

1.4.10.1 The contractor shall retrieve all identification media (including vehicle passes) from its employees who depart employment for any reason. The contractor shall return all identification media (i.e., badges and vehicles passes) to the KO within 14 days of an employee's departure.

1.4.11. Combating Trafficking in Persons: The United States Government has adopted a zero-tolerance policy regarding trafficking in persons. Contractors and contractor employees shall not engage in severe forms of trafficking in persons during the PoP of the contract; procure commercial sex acts during the PoP of the contract; or use forced labor in the performance of the contract. The Contractor shall notify its employees of the United States Government's zero-tolerance policy, the actions that will be taken against employees for violations of this policy. Such actions may include, but are not limited to, removal from the contract, reduction in benefits, or termination of employment. The Contractor shall take appropriate action, up to and including termination, against employees or subcontractors that violate the US Government policy as described at FAR 22.17.

1.4.12 Contractor Travel: Travel under this contract is not anticipated outside Fort Indiantown Gap. Limited movement to other buildings on the installation may be required to support CIF operations, attend meetings, or obtain Government-furnished materials. Any travel requiring reimbursement shall be specifically authorized in advance by the KO.

1.4.13 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.

1.4.14 Organizational Conflicts of Interest (OCI): The contractor and subcontractor personnel performing services 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 OCIs, 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 the KO. In the event the KO unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the KO may impose other remedies as he or she deems necessary, including prohibiting the contractor from participating in subsequent contracted requirements which may be affected by the OCI.

1.4.15 Phase In / Phase Out Periods: To minimize any decreases in productivity and to prevent possible negative impacts on services, the contractor shall have personnel on board during the phase in / phase out periods. During the phase in period, the contractor shall become familiar with performance requirements in order to commence full performance of services on the contract start date.

2.0 Definitions and Acronyms:

2.1 Definitions:

2.1.1 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.

2.1.2 Defective Service: A service output that does not meet the standard of performance associated with the PWS.

2.1.3 Deliverable: Anything that can be physically delivered and includes non-manufactured things such as meeting minutes or reports.

2.1.4 Key Personnel: Contractor personnel that are evaluated in a source selection process and that may be required to be used in the performance of a contract by the PWS. When key personnel are used as an evaluation factor in best value procurement, an offer can be rejected if it does not have a firm commitment from the persons that are listed in the proposal.

2.1.5 Physical Security: Actions that prevent the loss or damage of Government property.

2.1.6 Quality Assurance: The Government procedures to verify that services being performed by the Contractor are performed according to acceptable standards.

2.1.7 Quality Assurance Surveillance Plan: An organized written document specifying the surveillance methodology to be used for surveillance of contractor

performance.

2.1.8 Quality Control: All necessary measures taken by the Contractor to ensure that the quality of an end product or service shall meet contract requirements.

2.1.9 Subcontractor: One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

2.2 Acronyms:

AR	Army Regulation
AT/OPSEC	Antiterrorism/Operational Security
CAC	Common Access Card
CIF	Central Issuing Facility
CM	Contract Manager
COR	Contracting Officer Representative
CUI	Controlled Unclassified Information
DA	Department of the Army
DEERS	Defense Enrollment Eligibility Reporting System
DoD	Department of Defense
FAR	Federal Acquisition Regulation
FTIG	Fort Indiantown Gap
GFP/M/E/S	Government Furnished Property/Material/Equipment/Services
HQDA	Headquarters, Department of the Army
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IS	Information System(s)
KO	Contracting Officer
NGB	National Guard Bureau
OCIE	Organizational Clothing and Individual Equipment
OCI	Organizational Conflict of Interest
OPSEC	Operations Security
PAARNG	Pennsylvania Army National Guard
PII	Personally Identifiable Information
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QASP	Quality Assurance Surveillance Plan
QCP	Quality Control Program
RAPIDS	Real-Time Automated Personnel Identification System
SAM	System for Award Management
SOP	Standard Operating Procedure
TASS	Trusted Associate Sponsorship System
TE	Technical Exhibit
TARP	Threat Awareness and Reporting Program
USPFO	United States Property and Fiscal Office
OCONUS	Outside the Continental United States

3.0 Government Furnished Property, Material, Equipment and Services

(GFP/M/E/S):The Government will provide the property, material, equipment, and/or services listed below solely for the purpose of performance under this contract:

3.1 Property: The Government will furnish the necessary workspace for the contractor to perform services outlined in this PWS to include desk space, telephones, computers, counters, storage access, and other items necessary to maintain a CIF support work environment.

3.2 Materials: The Government will provide forms, locally required transaction documents, labels, bins, storage materials, packing materials, and other Government-owned items associated with CIF issue, exchange, turn-in, receiving, and storage operations.

3.3 Equipment: The Government will provide access to Government-owned systems, scanners, hand trucks, carts, shelving, forklifts or material handling equipment when required and authorized, and other equipment normally used in CIF operations. Contractor personnel shall meet any training or licensing requirements before operating Government equipment.

3.4 Services: The Government will provide access to applicable Government systems, maintenance support for Government-furnished equipment, and coordination with CIF, supply, and security personnel as required to enable contract performance.

3.5 Utilities: All utilities in the facility will be available for the contractor's use in the performance of this contract. The contractor shall instruct employees in utilities conservation practices. The contractor shall operate under conditions that preclude the waste of utilities.

4.0 Contractor Furnished Property, Materials, and Equipment (CFP/M/E):

4.1 General: Except for those items specifically stated to be Government-Furnished in Paragraph 3.0, the contractor shall furnish everything required to perform these services as indicated in Paragraph 1.1.

4.2 Contractor Security Clearance: N/A.

5.0 Requirements: The contractor shall:

5.1 CIF Support Servcies: The Contractor shall be responsible to provide the following services to support the United States Property and Fiscal Office (USPFO) and the Pennsylvania Army National Guard (PAARNG) Central Issuing Facility (CIF) with the execution of issue, exchange, turn-in, records, warehouse, and customer service support functions.

5.1.1 CIF Support services will supporting day-to-day CIF operations. The Contractor shall be responsible for supervision, scheduling, internal work assignment,

and quality control of assigned personnel. Contractor personnel shall not supervise Government employees, obligate Government funds, certify accountable records, or perform inherently governmental functions.

The Contractor shall maintain staffing continuity sufficient to meet mission requirements during normal duty hours, cross-train personnel to minimize service disruption, and provide qualified replacement personnel when vacancies, absences, or turnover affect performance. Selective consideration of the difficulty and requirements of assignments and capabilities of employees. Advises, counsels, and/or instructs the employees on both work and administrative matters.

5.1.2 Customer Service Support: Serve as points of contact for Soldiers, units, and supported activities with CIF service requirements. Receive customers, review documents for completeness, explain service requirements, manage customer flow, and resolve routine service problems related to CIF issue, exchange, and turn-in actions.

5.1.3 Issue and Turn-In Support: Perform OCIE issue, exchange, and turn-in processing in accordance with applicable Government procedures and locally approved CIF processes. Support high operational tempo periods, mobilization/demobilization events, Rapid Fielding Initiative (RFI) issue support, and other Government-directed CIF surge requirements.

5.1.4 Sizing and Fitting Support: Perform sizing and fitting of OCIE and related equipment, prepare customer issue packets, and ensure items are assembled for issue in accordance with applicable Government procedures and local CIF standards.

5.1.5 All specialists will review customer requests, appointment documents, hand receipts, and supporting records for completeness and accuracy before processing actions.

5.1.6 All specialists will identify discrepancies in quantities, records, condition, sizes, missing items, or supporting documentation and promptly elevate unresolved issues to the COR or designated Government official for decision.

5.1.7 All specialists will use approved Government systems and locally approved automated tools to enter, retrieve, update, and track CIF-related data required for performance of this contract.

5.1.8 All specialists will maintain supporting documentation for transaction packets, receipt and issue records, turn-in records, pending actions, and other required CIF files in an organized and audit-ready condition.

5.1.9 All specialists will provide copies or printouts of current records, transaction documents, and customer support documents to supported personnel and Government officials when requested.

5.1.10 All specialists will establish and maintain appointment rosters, suspense files, and local control logs used to track issues, exchanges, turn-ins, discrepancies, customer actions, and pending research.

5.1.11 All specialists will generate and submit reports as required to the COR on customer volume, issue actions, turn-ins, discrepancies, backlog status, and other workload indicators affecting mission performance.

5.1.12 All specialists will receive, review, and verify all requests for issue, exchange, partial turn-in, full turn-in, and record correction actions to ensure required approvals and authorizations are present.

5.1.13 All specialists will identify nonstandard, damaged, or unresolved item discrepancies and coordinate with the appropriate Government official for further review, disposition, or decision. All specialists will not make final Government determinations regarding liability, property disposition, or accountable record certification.

5.1.14 All specialists will verify and process customer receipts for OCIE and related items in accordance with applicable Army regulations, local CIF procedures, and Government-directed business rules. Maintain suspense document files for all transactions.

5.1.15 All specialists will maintain appropriate spreadsheets and track the status of due-ins, backorders, pending turn-ins, discrepancy research, and other CIF actions as directed by the COR.

5.1.16 All specialists shall review and assist with reconciliations between physical stock, customer records, transaction documents, and locally maintained control logs.

5.1.17 All specialists will track OCIE transactions, customer service statistics, and other Government-directed management data on spreadsheets or automated reports when required.

5.1.18 All specialists will provide technical support for CIF operations to include customer assistance, answering questions on CIF-related issues, and resolving routine discrepancies within the scope of contractor performance.

5.1.19 All specialists will assist in maintaining clean, orderly, safe, and mission-ready work areas within assigned CIF workspaces, issue counters, and storage areas.

5.1.20 All specialists will perform duties at BLDG 14-12, Fort Indiantown Gap, and may be required to move within the installation to obtain supplies, attend meetings, or support related CIF functions.

5.1.21 Services will be provided at the following location and for the requested man hours;

5.1.21.1 4,160 hours will be conducted at Building 14-12, Fort Indiantown Gap, for CIF Support Specialists.

5.1.21.2 Specialists will be trained and proficient in CIF operations.

5.1.21.3 Specialists shall support the full range of CIF operations during normal duty hours.

5.1.21.4 The Contractor shall cross-train personnel to ensure continuity of service and uninterrupted performance.

5.1.21.5 No dedicated team lead position is required under this PWS.

5.2 Issue and Turn-In Processing (applies to all specialists)

5.2.1 The contractor shall prepare, review, and process issue, exchange, and turn-in documents and update automated or manual control records as required by applicable procedures.

5.2.2 The contractor shall inspect items presented for issue or turn-in for serviceability, completeness, cleanliness, and correct size or configuration in accordance with local CIF standards and Government-furnished procedures.

5.3 Customer Records and Documentation (applies to all specialists)

5.3.1 The contractor shall receive and process customer record updates and transaction documents and ensure required supporting documents are complete and properly filed.

5.3.2 The contractor shall maintain suspense files for pending CIF actions.

5.4 Warehouse and Storage Support (applies to all specialists)

5.4.1 The contractor shall receive, stage, store, issue, exchange, and turn in items within assigned CIF areas and ensure items are placed in designated storage locations.

5.4.2 The contractor shall support surge issue and turn-in operations during mobilization, demobilization, deployment preparation, annual inventory periods, and other mission-driven workload increases.

5.4.3 The contractor shall segregate serviceable, unserviceable, and pending-disposition items and report stock discrepancies, unsafe conditions, or damaged items

to the Government.

5.5 Inventories and Reconciliations (applies to all specialists)

5.5.1 The contractor shall validate items received against receipt documents. When items received do not match the receipt document, the contractor shall report the discrepancy and prepare supporting documentation for Government review in accordance with local procedures.

5.5.2 The contractor shall support cyclic inventories, location surveys, document reconciliations, and audit-readiness efforts to help maintain accurate CIF stock records and supporting documentation.

5.6 Additional Requirements and notes (applies to all specialists):

5.6.1 Contractor personnel shall have demonstrated practical experience with logistics, warehouse, supply, retail issue, or CIF-type support operations. The Contractor assumes full responsibility and costs for ensuring fully qualified and trained personnel during the term of the contract.

5.6.1.1 Possess Army experience/knowledge directly related to CIF, OCIE, supply, or warehouse support requirements; experience with military clothing issue operations is preferred.

5.6.1.2 Have working knowledge of Army Regulations, procedures, and current policies pertaining to CIF operations, records management, customer service, and Army correspondence.

5.6.2 Contractor personnel shall be able to understand all regulations and directions applicable to CIF support services.

5.6.3 Contractor personnel shall have and maintain a valid driver’s license.

5.6.4 Contractor personnel shall have computer skills using Microsoft Office Suite including, but not limited to, Word, Excel, and Outlook.

5.6.5 Contractor personnel shall be physically capable of standing for extended periods, moving throughout storage areas, and handling OCIE and related items in accordance with local safety requirements.

5.6.6 Services will be performed on-site. Work hours may vary based on operational tempo. For reference, federal employees average 40 hours per week.

5.6.7 CIF Support Specialists will have a primary location of work as follows:

a. Building 14-12, Fort Indiantown Gap, Annville, PA 17003.
b. Additional temporary duty locations on Fort Indiantown Gap may be used only when required to support CIF mission operations.

5.6.8 The contractor personnel will be provided with adequate facilities located at the CIF, including a workstation and chair, computer, telephone, expendable supplies, computer hardware and software (and support), internet/intranet/Local Area Network (LAN), and use of copier and printer, as available. All Government furnished supplies and equipment shall be for official use only.

5.6.9 The contractor and COR shall conduct an inventory of all Government furnished equipment within ten days of commencement. The contractor shall sign a receipt for all furnished equipment. The contractor and COR shall determine the working condition of all equipment. The Government will replace and/or repair any item not in working order.

5.6.10 Contractor personnel shall be clearly identified within Government workplaces to ensure that those interacting with contractor personnel are at all times aware they are not interacting with Government employees.

5.6.10.1 Contractor personnel that have access to Government email and other systems must have user identification that calls attention to their special status as the contractor's employee.

5.6.10.2 Contractor shall establish a clear chain of authority through which instructions, clarifications, and changes to contractor performance are communicated to contractor personnel.

5.6.10.3 Contractor shall be responsible at all times for the supervision of contractor personnel, including but not limited to, maintenance of personnel records, scheduling of personnel, development of duty rosters, and approval of leave.

5.7 Contract Reporting:

5.7.1 The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the United States Property & Fiscal Office Pennsylvania (USPFO-PA) Purchasing & Contracting (P&C) via a secure data collection site.

5.7.1.1 The government estimates 3,840 manhours will be required annually for this service.

5.7.2 The contractor shall completely fill in all required data fields using the following web address: https://sam.gov. Log in and select Entity Registrations and then select Service Contract Reporting.

The Contractor shall report the required information annually by October 31, for services performed under this contract during the preceding Government fiscal year (October 1-September 30).

The DoD Guidebook for Service Contract Reporting in SAM, available on the DoD Procurement Toolbox at https://dodprocurementtoolbox.com/site-pages/service-contract-reporting-scr. The General Services Administration (GSA) has also posted additional guidance such as quick start guides, informational videos, and frequently asked questions, that can be accessed by going to https://sam.gov and searching the "HELP" section. The SAM Federal User Guide is also available in the "HELP" section for comprehensive instructions on navigating SAM. Contractors requiring assistance using SAM should contact the Federal Service Desk at https://www.fsd.gov.

6.0 Applicable Publications: Publications applicable to this PWS are listed below:

Publication (Chapter/Page)	Date of Publication	Mandatory or Advisory	Website
Federal Acquisition Regulation	Not published	Mandatory	https://www.acquisition.gov/?q=browsefar
Defense Federal Acquisition Regulation Supplement	07/09/2021	Mandatory	http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html or https://www.acquisition.gov/dfars
Joint Travel Regulation (JTR)	03/01/2023	Mandatory	https://www.defensetravel.dod.mil/site/travelreg.cfm
DoDM 1000.13-M-V1 DoD Identification (ID) Cards(Enclosure 2, paragraph 3.b)	01/23/2014 (Change 1: 07/28/2020)	Advisory	http://www.esd.whs.mil/Directives/issuances/dodm
Federal Information Processing Standards (FIPS) Publication 201-3 Personal Identity Verification (PIV) of Federal Employees and Contractors (paragraph 9)	January 2022	Advisory	https://doi.org/10.6028/NIST.FIPS.201-3
DoDM 5200.2 Procedures for the Personnel Security Program (PSP)	04/03/2017	Advisory	https://www.esd.whs.mil/Directives/issuances/dodm/
DoDI 5200.46 DoD Investigative and Adjudicative Guidance for Issuing the CommonAccess Card (CAC)	09/09/14 (Change 2: 11/2/2020)	Advisory	https://www.esd.whs.mil/Directives/issuances/dodi/

Homeland Security Presidential Directive (HSPD)-12 Policy for a Common Identification Standard for Federal Employees and Contractors	08/27/2004	Advisory	www.dhs.gov/homeland-security-presidential-directive-12
DoDI 5400.11 Department of Defense Privacy and Civil Liberties Programs	01/29/2019 (Change 1: 12/8/2020)	Advisory	https://www.esd.whs.mil/Directives/issuances/dodi/
DoD 5400.11-R Department of Defense Privacy Program	05/14/2007	Advisory	https://www.esd.whs.mil/Directives/issuances/dodm/
DoDD 8140.01 Cyberspace Workforce Management	10/05/2020	Advisory	https://www.esd.whs.mil/Directives/issuances/dodd/
DoDM 8140.03 Cyberspace Workforce Qualification and Management Program	2/15/2023	Advisory	https://www.esd.whs.mil/Directives/issuances/dodm/
DoD 5220.22-M National Industrial Security Program Operating Manual (now Part 117 of Title 32, Code of Federal Regulations)	12/21/2020	Advisory	https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117
Army Directive 2014-05 Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors	03/07/2014	Advisory	nypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=10409_5
AR 25-2 Army Cybersecurity	04/04/2019	Mandatory	https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1002626
AR 530-1 Operations Security	09/26/2014	Mandatory	http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
AR 525-13 Antiterrorism	12/03/2019	Mandatory	http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
AR 381-12 Threat Awareness and Reporting Program (TARP) (Section II, ¶ 2-4.b)	06/01/2016	Mandatory	http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
AR 710-1 Centralized Inventory Management Of The Army	11/28/2016	Mandatory	apd.army.mil/ProducTMaps/PubForm/AR.aspx

Supply System			
AR 710-2 SECONDARY ITEM POLICY AND RETAIL LEVEL MANAGEMENT	07/01/2024	Mandatory	http://www.apd.army.mil/ProductMaps/PubForm/AR.aspx
AR 710-3 INVENTORY MANAGEMENT ASSET AND TRANSACTION REPORTING SYSTEM	09/02/2021	Mandatory	http://www.apd.army.mil/ProductMaps/PubForm/AR.aspx
AR 710-4 Inventory Management Property Accountability	01/26/2024	Mandatory	apd.army.mil/ProductMaps/PubForm/AR.aspx
AR 735-5 RELIEF OF RESPONSIBILITY AND ACCOUNTABILITY	03/10/2024	Mandatory	https://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
DA PAM 710-2-1 Using Unit Supply System (Manual Procedures)	12/1/2016	Mandatory	http://www.apd.army.mil/ProductMaps/PubForm/PAM.aspx
DA PAM 735-5 Property Accountability Procedures and Financial Liability Officers Guide	03/23/2016	Mandatory	http://www.apd.army.mil/pdffiles/r40_5.pdf
PMR 525-2 PANG Protection Program	10/03/2022	Mandatory	Pennsylvania G3/4 - PMR 525-2Updated 3 OCT 2022.pdf - All Documents (sharepoint-mil.us)
AR 700-84 Issue and Sale of Personal Clothing	03/26/2025	Mandatory	https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN39779-AR_700-84-000-WEB-1.pdf

6.1 Applicable Forms: Forms applicable to the PWS are listed below:

Form	Date	Website
DA Form 4949 Administrative Adjustment Report	01/1/1982	https://armypubs.army.mil/ProductMaps/PubForm/DAForm4 001_5000.aspx
DD 1172-2 Application for Identification Card/DEERS Enrollment	04/24/2020	https://www.esd.whs.mil/Directives/forms/dd1000_1499/DD1 172-2/
I-9 Employment Eligibility Verification	08/01/2023	https://www.uscis.gov/sites/default/files/files/form/i-9.pdf
DD 441 Department of Defense Security Agreement	03/01/2020	https://www.esd.whs.mil/Directives/forms/dd0001_0499/

DD 250 Material Inspection and Receiving Report	08/01/2000	https://www.esd.whs.mil/Directives/forms/dd0001_0499/
DA Form 1687 NOTICE OF DELEGATION OF AUTHORITY - RECEIPT FOR SUPPLIES	12/01/2023	https://armypubs.army.mil/ProductMaps/PubForm/DAForm10 01_2000.aspx
DA Form 3161 REQUEST FOR ISSUE OR TURN-IN	12/01/2023	https://armypubs.army.mil/ProductMaps/PubForm/DAForm30 01_4000.aspx
DA FORM 2062 HAND RECEIPT/SHORTAGE LISTING	12/01/2023	https://armypubs.army.mil/default.aspx
	06/01/2023	https://armypubs.army.mil/default.aspx

TECHNICAL EXHIBIT 1

Performance Requirements Summary (PRS)

This PRS includes performance objectives the Government will use to determine contractor performance and will compare contractor performance to the Acceptable Quality Level (AQL).

Performance Objectives	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method & By Whom
Contractor shall process CIF issue, exchange, and turn-in actions accurately. PWS Para 5.1, 5.2, 5.3, 5.4, & 5.5.	Issue, exchange, and turn-in documents and supporting entries are accurate with less than 2 errors out of every 100 transactions.	Less than 2 errors out of every 100 transactions	Sample Check by COR and designated Government CIF staff Daily or when required due to operational tempo
Contractor shall maintain accurate customer records, suspense files, and supporting documentation. PWS Para 5.1, 5.2, 5.3, 5.4, & 5.5.	Customer records, suspense files, and transaction packets are complete, current, and properly filed within three (3) workdays of generation or receipt.	No more than five (5) instances of incorrect filing per month	Sample Check by COR and designated Government CIF staff Monthly

Reports, spreadsheets, and management data are complete and contain no errors that would lead the intended recipient to draw faulty conclusions. PWS Para 5.1, 5.2, 5.3, 5.4, & 5.5.	100% error free reports, spreadsheets, and briefing documents.	0% failure is acceptable	Reviewed by COR as required
Contractor shall support issue, turn-in, and warehouse operations in accordance with local CIF procedures. PWS Para 5.1, 5.2, 5.3, 5.4, & 5.5.	Items are properly staged, stored, issued, or turned in, and discrepancies are reported within one workday.	95% compliance	Sample Check by COR and designated Government CIF staff Weekly
Contractor shall provide timely customer service support. PWS Para 5.1, 5.2, 5.3, 5.4, & 5.5.	Customers are processed courteously and professionally and routine transactions are completed without justified complaint.	95% compliance	COR observation / customer feedback Monthly
Maintain Suspense and Supporting Document Files. PWS Para 5.2, 5.3, 5.4, & 5.5	Documentation is properly filed within three (3) workdays of generation or receipt.	No more than five (5) instances of incorrect filing per month	Sample Check by COR Monthly.
Review & Assist with Reconciliations. PWS Para 5.1.15	Review stock, location, and transaction records for accuracy and assist with monthly cyclic inventories and reconciliations.	Less than 2 errors out of every 100 reconciliations is acceptable	COR and designated Government CIF staff Monthly.
Track Customer Volume / OCIE Transactions. PWS 5.1.16	Customer volume, issue, exchange, and turn-in transactions will be tracked accurately on Government-directed spreadsheets or reports with less than 2 errors out of every 100 entries.	Less than 2 errors out of every 100 transactions related to data entry information is acceptable.	COR Prior to monthly reporting.

TECHNICAL EXHIBIT 2

Deliverables Schedule

erence / Deliverable Title	Frequency	umber of Copies	Medium/ Format	Submit To
1.4.5.1.5 / Receipt for each CAC card returned to the DEERS office.	Within 15 calendar days of returning issued CACs to the DEERS office upon departure or dismissal of each contractor employee	1	Electronic Submission	TA/COR
1.4.5.3 / AT Level 1 Awareness Training Certificates	Provide within 15 calendar days after employee completes training.	1	Electronic Submission	COR
1.4.5.4 / iWATCH Training Certificates	Provide within 15 calendar days after employee completes training.	1	Electronic Submission	COR
1.4.5.11 / OPSEC Training Certificates	Provide within 15 calendar days after employee completes training.	1	Electronic Submission	COR
1.4.3 / Quality Control Plan	Within 10 calendar days after contract award	1	Electronic Submission	KO/COR
1.4.10 / Identification Media	Return within 14 days of employee's departure from contract performance.	Original(s)	Hard Copy	KO
5.1, 5.2, 5.3, 5.4, & 5.5 / Provide CIF support services	Daily and/or as required by the COR	1	Automated / Electronic/SEAM	COR
5.2 / Process issue, exchange, and turn-in documents	At the conclusion of the process / transaction	1	Automated / Electronic/SEAM	COR
5.2, 5.3, 5.4, & 5.5 / Maintain suspense and supporting document files	Daily and/or as required by the COR	1	Electronic and paper copy backup	COR
5.1.15 / Review & Assist with Reconciliations	Monthly	1	Automated / Electronic and paper copy backup	COR

5.1.16 / Track customer volume and OCIE transactions	Monthly	1	Government-directed spreadsheet / report/SEAM	COR

TECHNICAL EXHIBIT 3

Estimated Workload Data

This information is provided for historical background only. It is not a guarantee of workload quantities.

ITEM	DESCRIPTION	ESTIMATED QUANTITY
1	CIF support services to be conducted at Fort Indiantown Gap (FTIG), PA.	CIF support services are estimated to require 3,840 manhours. Locationed at BLDG 14-12, FTIG, provide issue, exchange, turn-in, records, warehouse, and customer service support during normal duty hours.
2	Customer issue / exchange transactions.	Estimated quantity: Averaging around 950 FLIP transactions per year.
3	Customer turn-in transactions.	Estimated quantity: Averaging 178 turn-ins transactions a month.
4	Inventory / reconciliation and warehouse support actions.	Estimated quantity: Once per year and 15 days to complete inventory.

//END OF PERFORMANCE WORK STATEMENT//