PERFORMANCE WORK STATEMENT (PWS)

1.0 General:

1.1 Scope: The contractor shall provide a realistic replicated information environment for the Cyber Yankee 2023 exercise. This includes support preparing for the exercise, training, and onsite support for the event.

1.1.1 Objectives**:** The objective is to obtain a realistic replicated information environment for the Cyber Yankee 2023 exercise from May 13-26, 2023. Replicating the internet, including social media applications and other traditional media, allows for a more dynamic training scenario for participants and aids in the training areas such as emergency response, open-source intelligence, best practices for public communication best practices, interagency coordination, and defensive cyber operations.

1.2 Background: The intent of Cyber Yankee 2023 is to provide a realistic cyber exercise to assess cyber teams from state Army National Guard Defensive Cyberspace Operations Elements (DCOE), Air National Guard Joint Forces Headquarters elements, and other participating Army and Air National Guard, Coast Guard, Air Force and Navy Reserve Cyber Elements. To achieve this intent, we will design a dynamic training environment to allow the training audience to have flexibility and variation in training objectives/goals. A realistic scenario with replicated conditions intelligence analysists would face is a critical component of ensuring the readiness of DCOE teams.

1.3 Period of Performance (PoP): The Period of Performance shall be 1 April to 26 May 2023.

1.4 General Information:

1.4.1 Place and Performance of Services: The contractor shall performance services remotely and at Camp Nett at Niantic, Connecticut. The contractor shall at all times maintain an adequate work force for the uninterrupted performance of all tasks defined within this PWS.

1.4.1.1 Telework is not authorized.

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 Contractor Travel: The contractor shall travel to Niantic, Connecticut during the performance of this contract to attend meetings and the Cyber Yankee 2023 exercise. The contractor will be not authorized travel expenses by the Government.

1.4.2 Recognized Holidays: The following are recognized United States (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 National Independence Day: 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: December 25th

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.

1.4.4 Quality Assurance (QA): The Government 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 Government will 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 RESERVED

1.4.5.1.1 RESERVED

1.4.5.1.2 RESERVED

1.4.5.1.3 RESERVED

1.4.5.1.4 RESERVED

1.4.5.1.5 RESERVED

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 using the National Crime Information Center Interstate Identification (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05), 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/atl1/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 RESERVED

1.4.5.6.1 RESERVED

1.4.5.6.2 RESERVED

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 RESERVED

1.4.5.8 RESERVED

1.4.5.9 RESERVED

1.4.5.10 RESERVED

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 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 RESERVED

1.4.5.13 RESERVED

1.4.5.14 RESERVED

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 RESERVED

1.4.6.1.1 RESERVED

1.4.6.1.2 RESERVED

1.4.6.1.3 RESERVED

1.4.6.2 RESERVED

1.4.7 Special Qualifications: The contractor shall ensure all employees possess all required licenses for operating equipment used in the performance of this contract. This does not include education or other qualifications for the position in which the contractor employee is performing, dress codes, or other information. (NOTE: The Government does not provide training to contractors. Contractors must ensure that any personnel performing under a contract are fully trained, licensed, certified, and otherwise qualified to provide services).

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 FAR 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 KO 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.

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

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 period of performance of the contract; procure commercial sex acts during the period of performance 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. 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 RESERVED

1.4.13 Data Rights The Government has unlimited rights to all documents/materials 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 participation in subsequent contracted requirements which may be affected by the OCI.

1.4.15 RESERVED

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 (QASP): 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:

AEI	Army Enterprise Infostructure
AR	Army Regulation
AT/OPSEC	Antiterrorism/Operational Security
BI	Background Investigation
CM	Contract Manager
COR	Contracting Officer Representative
DA	Department of the Army
DD254	Department of Defense Contract Security Classification Specification
DFARS	Defense Federal Acquisition Regulation Supplement
DoD	Department of Defense
DSCA	Defense Counterintelligence and Security Agency
FAR	Federal Acquisition Regulation
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
OCI	Organizational Conflict of Interest
PII	Personally Identifiable Information
PIPO	Phase In/Phase Out
POC	Point of Contact
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Program
SCR	Service Contract Reporting
SSN	Social Security Number
TE	Technical Exhibit
USD(I)	Under Secretary of Defense for Intelligence

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: None

3.2 Materials: None

3.3 Equipment: None

3.4 Services: None

3.5 Utilities: All utilities in the facility will be available for the contactor'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, which include turning off the water faucets or valves after using the required amount.

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 Secret Facility Clearance: None

4.3 Contractor Security Clearance: None

5.0 Requirements: The contract shall provide:

5.1 **Single-Exercise License**: The single-exercise event license will provide access to the cloud-based application for the planning, design, replication of the internet, including social media applications and traditional media sites for one exercise event in the current Persistent Cyber Training Environment (PCTE) Platform.

5.1.1 Accessibility: The Contractor will make available via any internet-connected mobile device or computer to prepare participants for the exercise. The access should validate participants to the platform and familiarize participants with the information environment that will be used during execution.

5.2 **Technical Specifications:** The Contractor will monitor the platform with system administrators who can anticipate and mitigate potential problems. A technical support team will be available to troubleshoot, answer questions, and provide user guidance for the duration of the exercise. The contractor will provide a HSEEP-Based, Password protected application with the ability for Cyber Yankee Range Team Controllers to upload videos, print stories, photographs, blogs, and other posts on pages that look and function like mainstream and social media sites. The PCTE is the primary distribution point for exercise media products. The Contractor will provide a kernelized solution to prevent data from crossing over from one "firewalled" exercise to another. A Web interface with user account controls for file management to allow non-technical personnel (Exercise Controllers and exercise participants) to upload content with ease.

5.2.1 Required Scalability: The contractor's solution will provide scalability to support Cyber Yankee Industrial sector in scope from a single venue event with 20 user accounts. The Contractor software will allow various types of mainstream media, social media and government/agency pages to cross post and share content similar to the functions of existing Web-based agency home pages, mainstream media and social media sites.

5.2.2 Required Notifications: The contractor's solution will provide automatic notifications when new content is posted to user accounts via PCTE environment and Mobile Application. Simulations must be clearly marked "For Exercise Purposes Only" to protect operational security and prevent exercise scenarios from being alerted to Army Cyber Command via "Cyber 9 line" content.

5.2.3 Required Security Features: Industry and Government best practices to ensure security of information, which included but is not limited to hosting on an "HTTPS" Server; providing password protected accounts and incorporate measures to prevent audio, video, and imagery content from being downloaded and distributed out of context. The Contractor's solution in PCTS must conform to HTML 5 standards, which allows all devices (computer, mobile, etc.) to access video, as opposed to Flash-based systems that are not universally accessible and acceptable. All Audio and Video Files uploaded to the platform are not downloadable in accordance with DHS IT security guidelines.

5.2.4 Required On-Site Exercise Liaison for Execution: The on-site exercise liaison for execution will lead the implementation of the training exercise and coordinate exercise control, evaluation, facilitation, as well as simulation and after-action reporting. The liaison will plan and manage the replicated information environment for the exercise play and sustain the pace of the exercise.

5.3 Delivery and Setup: Installation of all scenarios in to the PCTE environment must occur not later than 15 April 2023 working directly with our PCTS Operators. All Simulation Injects shall be delivered withing PCTE no later than (5) days upon notification of award, the contractor shall provide a single Project Manager for NHARNG personnel to contact regarding all facets of the installation phase. Where this will be the Contractor's designated Contract Manager (CM), it is not required; however, this person should be cognizant of the entire installation and integration process and be empowered to make decisions that affect it. The awarded vendor must be able to produce a series of tools and templates based on the standards and principles published and maintained by the Project Management Institute (PMI). The awarded vendor is required to produce the following deliverables (templates): Project strategy, Project Schedule, Status Reports, Account Management, SLA performance, Risk Management, on-boarding process, contracted deliverables. The Contract Manager will coordinate with the incumbent for all coordination with Cyber Yankee. During the Cyber Yankee Event the Contractor shall update and provide daily, to the White Cell director, all progress relative to the daily exercise schedule, ensuring to highlight any deviance from original plan; this

to ensure that no injects go lost. Immediately upon availability and determination, the Contractor shall provide verbal reports to White Cell Exercise Director and the Contracting Office. Also required is any username and passwords for all 150 users for web/mobile interface purposes. The Contractor will incorporate this information into the requirement for an estimated delivery schedule at their discretion; however, should not delay the provision of any information if otherwise required information is unavailable. At the Contractor's expense (without reimbursement provisions), pre-installation visits may be conducted. To accomplish, the Contractor must coordinate with the 'Key Operator' for Cyber Yankee, to be designated and provided by the White Cell Exercise Director upon award. Upon completion of Cyber Yankee, the Contractor shall provide a report for the After-Action Review that summarizes all injects, by platform and device in support of this contract. In person, on-site familiarization is not required.

5.4 Maintenance/Service/Support Agreement: The support team will assist the on-site exercise liaison with exercise control, to include prompts or initiation of actions to ensure exercise continuity and flow. Additionally, the support team will provide guidance on training and assist with technical support as needed. *Planning Support:* The contractor will work with the exercise staff leading up to the exercise to coordinate efforts. This includes synchronizing with the intel, red team, and range team to match the replicated social media environment with the scenario and injects that teams will be evaluated on. Planning support will include development of the replicated information environment to include social media, blogs and photo/video sites. The service agreement in place must ensure intellectual property that transmits analogue sites to real-world media sites do not infringe upon copyright or other legal protections that apply to commercial sites.

5.5 Backup: The Contractor will ensure backups are automatic and continuous at one-minute intervals to ensure continuity of data during the Cyber Yankee Exercise. Note-Taking feature will be available and accessible to Exercise Controllers in order to enter time-stamped observations in real time and export observations for inclusion in the After Action Report.

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

Publication (Chapter/Page)	Date of Publication	Mandatory or Advisory	Website
Federal Acquisition Regulation			https://www.acquisition.gov/?q=browsefar
Defense Federal Acquisition Regulation Supplement			http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html or https://www.acquisition.gov/dfars
Joint Travel Regulation (JTR)			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)		http://www.esd.whs.mil/Directives/issuances/dodm
Federal Information Processing Standards (FIPS) Publication 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors (paragraph 9)	August 2013		http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
DoDM 5200.2 Procedures for the DoD Personnel Security Program (PSP)	04/03/2017		https://www.esd.whs.mil/Directives/issuances/dodm/
DoDI 5200.46 DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)	09/09/14 (Change 1: 05/04/2018)		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		https://www.dhs.gov/homeland-security-presidential-directive-12
DoDI 5400.11 Department of Defense Privacy and Civil Liberties Programs	01/29/2019		https://www.esd.whs.mil/Directives/issuances/dodi/
DoD 5400.11-R Department of Defense Privacy Program	05/14/2007		https://www.esd.whs.mil/Directives/issuances/dodm/
DoDD 8140.01 Cyberspace Workforce Management	10/05/2020		https://www.esd.whs.mil/Directives/issuances/dodd/
DoD 8570.01-M Information Assurance Workforce Improvement Program	12/19/2005 (Change 4: 11/10/2015)		https://www.esd.whs.mil/Directives/issuances/dodm/
DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM)	02/28/2006 (Change 2: 05/18/2016)		https://www.esd.whs.mil/Directives/issuances/dodm/
Army Directive 2014-05 Policy and Implementation Procedures for Common Access Card Credentialing and Installation Access for Uncleared Contractors	03/07/2014		https://armypubs.army.mil/ProductMaps/PubForm/ArmyDir.aspx
AR 25-2 Information Assurance	04/04/2019		http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
AR 530-1 Operations Security	09/26/2014		http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx
AR 525-13 Antiterrorism	12/09/2019		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		http://armypubs.army.mil/ProductMaps/PubForm/AR.aspx

6.1 Additional Applicable References:

Federal Information Processing Standards Publication 140-2, updated December 3, 2002	**https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf**
Trade Agreement Act Compliance	**http://gsa.federalschedules.com/resources/taa-designated-countries/**
Defense Information Service Agency Security Technical Implementation Guides (STIGs)	**https://iase.disa.mil/stigs/Pages/index.aspx**
Army CHESS ITES-3H contract	**Mps://chess.army.mil/Contract/Ites3H**
Army Records Information Management System	**htpps://www.arims.army.mil**
Interactive Personnel Electronic Records Management System	**https://iperms.hrc.army.mil**
Army Directive 2013-26, 2 December 2013, Subject: Army-wide Management of Printing and Copying Devices	**https://armypubs.army.mil/ProductMaps/PubForm/ArmyDir.aspx**
U.S. Army Audit Agency Audit Report A-2010- 0091-FFI (Copier Management), 26 April 2010	**https://www.aaa.army.mil**
U.S. Army Audit Agency Audit Report A-2012- 0113-FMT (Printer Management), 31 May 2012	**https://www.aaa.army.mil**
Executive Order 13589, 9 November 2011, Subject: Promoting Efficient Spending	**https://obamawhitehouse.archives.gov/the-press-office/2011/11/09/executive-order-13589-promoting**
Memorandum, Department of Defense Chief Information Officer, 17 February 2012, Subject: Optimizing Use of Employee Information Technology (IT) Devices and Other Information Technologies to Achieve Efficiencies	**http://dodcio.defense.gov**
Army Regulation 25-1 (Army Information Technology), 25 June 2013	**https://www.army.mil/usapa/epubs/pdf/r25 1.pdf**

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 Objective	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method / By Whom
5.0 Single-Exercise License	The contractor shall ensure users that require access to the platform are registered ahead of the exercise start date.	Unlimited Access during PoP	Random Sampling / COR
5.1 Accessibility	The contractor shall ensure the solution will be made available on any internet based platform during the exercise.	Unlimited Access during PoP	Periodic Inspection / COR
5.1.4 On-Site Exercise Liaison for Execution	The liaison shall plan and manage the replicated information environment for the exercise play and sustain the pace of the exercise.	80 hours	Customer Feedback / COR
5.2 Delivery Setup	A technical support team will be available to setup, troubleshoot, answer questions, and provide user guidance for the duration of the exercise.	Unlimited Access during PoP	Customer Feedback / COR
5.3 Support Team for Execution	The support team shall assist the on-site and planning process exercise liaison with exercise control, to include prompts or initiation of actions to ensure exercise continuity and flow.	180 hours	Customer Feedback / COR
5.4 Backup	The contractor will ensure backups are automatically and continuous.	Unlimited During Exercise	Periodic Inspection / COR