HIGH PERFORMANCE COMPUTER MODERNIZATION PROGRAM (HPCMP)

CYBERSECURITY SERVICE PROVIDER (CSSP) SUPPORT SERVICES

RFP
W912HZ22R0007
AMENDMENT 0005
19 DECEMBER 2022

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
J	1 | 58

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO.(If applicable)
0005	19-Dec-2022		

6. ISSUED BY	CODE	7. ADMINISTERED BY (If other than item 6)	CODE
ERDC CONTRACTING OFFICE 3909 HALLS FERRY ROAD VICKSBURG MS 39180-6199	W912HZ	See Item 6	

8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and Zip Code)		
	X	9A. AMENDMENT OF SOLICITATION NO. W912HZ22R0007
	X	9B. DATED (SEE ITEM 11) 26-Sep-2022
		10A. MOD. OF CONTRACT/ORDER NO.
		10B. DATED (SEE ITEM 13)
CODE / FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

[X] The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offer [ ] is extended, [X] is not extended.

Offer must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended by one of the following methods: (a) By completing Items 8 and 15, and returning 1 copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS.
IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

[ ] A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.

[ ] B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(B).

[ ] C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

[ ] D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor [ ] is not, [ ] is required to sign this document and return _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this Amendment is to make the following changes:

1. Update Solicitation Section PWS, as noted by changes marked as AM#0005.
2. Update Solicitation Section L, as noted by changes marked as AM#0005.
3. Incorporate the Government responses to ProjNet Inquiries submitted by potential offerors Between 17-Nov-22 and 14-Dec-22, with Attachment 1.
4. Update RFP Attachment 5 Price Proposal Template 20221215-REV-3 Amend 0005.
5. All other terms and conditions remain the same.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) TEL: EMAIL:	
15B. CONTRACTOR/OFFEROR _____ (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY _____ (Signature of Contracting Officer)	16C. DATE SIGNED 19-Dec-2022

SECTION SF 30 BLOCK 14 CONTINUATION PAGE

SUMMARY OF CHANGES

SECTION C - DESCRIPTIONS AND SPECIFICATIONS

The following have been modified:
PWS

Performance Work Statement (PWS)
HPCMP CSSP Contract

Table of Contents

1 Introduction

The primary purpose of this Performance Work Statement (PWS) is to acquire cybersecurity services in support of the High Performance Computing Modernization Program (HPCMP) Cybersecurity Service Provider (CSSP) mission to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks residing on the Defense Research Engineering Network (DREN) and the Secret DREN (SDREN). The HPCMP CSSP employs cybersecurity principals and includes deliberate actions taken to modify an assurance configuration or condition in response to a cybersecurity alert or threat information. The HPCMP CSSP helps organizations impacted by a cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state; respond to crises or urgent situations within the pertinent domain to mitigate immediate and potential application, system, or network threats; and perform security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.

1.1 Mission

The HPCMP manages the Department of Defense (DoD) Research, Development, Test, and Evaluation (RDT&E) network, the DREN, and its classified counterpart, the SDREN. As a component of the Department of Defense Information Network (DoDIN), the DREN and SDREN provide secure high performance wide area network services in support of DoD scientists and engineers, as well as other related DoD communities and Federal agencies.

1.2 Background

The Engineer Research Development Center (ERDC) Information Technology Laboratory (ITL) is the Executive Agent for the DoD HPCMP. The HPCMP is designated as an Area of Operation (AOR) within the DoDIN due to its operation and management of the DREN and SDREN. The HPCMP operates as a Tier 1 CSSP for the entirety of the DREN and SDREN, and as a Tier 2 CSSP for portions of the DREN and SDREN.

1.3 Scope

The HPCMP has the mission to protect and support the networks, information systems, and the confidentiality, integrity, and availability of the data on the DREN and SDREN. HPCMP provides comprehensive services for Identify; Protect; Monitor, Analyze, and Detect; Respond; and Sustainment functions to maintain a robust and consistent security environment in accordance with (IAW) current Evaluator Scoring Metrics (ESM) and DODI 8530.1, 7 MAR 2016. The HPCMP cybersecurity subscriber base at present includes 138 sites and ~35,000 hosts, which may vary +/- 10%. The HPCMP CSSP currently receives approximately 115,000 intrusion detection system (IDS) alerts per week. Of these alerts, the majority occur during core hours.

1.4 Period of Performance

The period of performance for this task order will be with a one (1) year base period of performance, four (4) one (1) year options and one (1) six (6) month extension of services option.

2 General Requirements

This section describes the general requirements the contractor needs to accomplish. The following sub-sections provide details of various considerations on this effort.

2.1 Non-Personal Services

The Government shall neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the contractor believes that any actions constitute, or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the Procuring Contracting Officer (PCO) immediately.

2.2 Business Relations

The contractor shall successfully integrate and coordinate all activity needed to execute the requirement. The contractor shall manage the timeliness, completeness, and quality of problem identification. The contractor shall

provide corrective action plans, proposal submittals, timely identification of issues, and effective management of subcontractors. The contractor shall seek to ensure subscriber satisfaction and professional and ethical behavior of all contractor personnel.

2.3 Contract Administration and Management

The following subsections specify requirements for contract, management, and personnel administration.

2.3.1 Contract Management

The contractor shall establish processes and assign appropriate resources to effectively administer the requirement. The contractor shall respond to Government requests for contractual actions in a timely fashion. The contractor shall have a single point of contact between the Government and Contractor personnel assigned to execute contracts or task orders. The contractor shall assign work effort and maintain proper and accurate time keeping records of personnel assigned to work on the requirement.

2.3.2 Contract Administration

The contractor shall establish processes and assign appropriate resources to effectively administer the requirement. The contractor shall respond to Government requests for contractual actions in a timely fashion. The contractor shall have a single point of contact between the Government and Contractor personnel assigned to support contracts or task orders. The contractor shall assign work effort and maintaining proper and accurate time keeping records of personnel assigned to work on the requirement.

2.3.3 Personnel Administration

The contractor shall provide the following management and support as required. The contractor shall provide for employees during designated Government non-work days or other periods where Government offices are closed due to weather or security conditions. The contractor shall maintain the currency of their employees by providing initial and refresher training as required to meet the PWS requirements. The contractor shall make necessary travel arrangements for employees. The contractor shall provide administrative support to employees in a timely fashion (time keeping, leave processing, pay, emergency needs).

The Contractor shall staff vacant positions within thirty (30) days of being vacant.

2.4 Subcontract Management

The contractor shall be responsible for any subcontract management necessary to integrate work performed on this requirement and shall be responsible and accountable for subcontractor performance on this requirement. The prime contractor will manage work distribution to ensure there are no Organizational Conflict of Interest (OCI) considerations. Contractors may add subcontractors to their team after notification and approval to the Procuring Contracting Officer (PCO) or Contracting Officer Representative (COR).

2.5 Contractor Personnel, Disciplines, and Specialties

The contractor shall build a quality culture that self-identifies problems or areas for improvement. The contractor shall strive to proactively identify problems, or potential issues, affecting performance and proactively work to resolve them. The contractor shall report these items to the COR as soon as possible. Verbal reports will be followed up with written reports when directed by the COR, or the contractor may submit a written report to identify the issue and how it was resolved in order to record these actions for the Government’s consideration. Identified discrepancies in which the contractor has proactively taken action to remedy the discrepancy and provide confidence of future compliance, the Government COR may determine that a formal task discrepancy report will not be issued. The contractor remains responsible to correct problems/issues that need resolution. The contractor shall work cooperatively with the Government to resolve issues as they arise.

2.5.1 Responsive Subscriber Service

The contractor shall respond to all tasks, questions, and inquiries from the COR and/or PCO by providing initial written acknowledgement within two (2) business days. All Government questions and inquiries shall be addressed and all tasks completed within the established Government timeframe. The contractor shall provide courteous and competent subscriber service and shall be flexible and responsive to the Government's evolving requirements or emergent activities.

2.5.2 Unacceptable Performance
Unless otherwise directed by the Government, the contractor shall immediately take action to correct or replace all non-conforming services or deliverables at no additional cost to the Government. If the contractor fails to perform at an acceptable quality level, the Government may issue a Task Discrepancy Report (TDR) to the contractor. The contractor shall complete their portion of the TDR and provide any supporting documents to support their response. The TDR response and supporting documents shall be submitted no later than the required due date established by the Government.

2.5.3 Removal of Personnel at Government Request
Contractor personnel do not work for the Government. However, in rare cases, the Government may request removal (permanent or temporary) of contractor personnel from performance of these requirements for security, safety, environmental, or health reasons, upon discovery of fraudulent qualification documentation, or when contractor personnel behave in an unprofessional manner that would be considered unacceptable by a reasonable person. The contractor shall ensure continuation of services such that impact to the Government is minimal and that replacements/substitutions comply with personnel competencies and personnel qualifications.

2.5.4 Standards of Conduct and Appearance
The contractor shall ensure that their employee policy for standards of conduct and personal appearance foster a professional and safe work environment that conforms to the Government's existing organizational culture and employee standards. Contractor employees who pose a threat to the safety or welfare of the installation or its personnel may be immediately removed and/or barred from the installation.

2.6 Location and Hours of Work

2.6.1 Place of Performance

The current on-site locations of performance are:

- ERDC, 3909 Halls Ferry Road, Vicksburg, Mississippi
- AFRL, Building 271, 2721 Sacramento Street, Dayton, Ohio
- HPCMPO, Kingman Building, Fort Belvoir, Virginia

The maximum seating capacity for each location is identified in Table 1.

Table 1: Maximum Seating Capacity

On-Site Location	Unclassified Maximum Seating	Classified Maximum Seating
ERDC	35[2]	24[1]
AFRL	10	10[1]
HPCMPO	4	3[1]

[1] These seats are "hot desks" that a contractor employee chooses upon arrival, and are in secure areas with access to classified AND unclassified workstations.
[2] Infrastructure Services and Program Manager sit in an unclassified space at ERDC.

(1) Program Manager (3.1). The contractor shall work on-site at ERDC.
(2) Detect Services (3.2). The contractor shall work on-site at ERDC and AFRL. Personnel located at HPCMPO is optional.
(3) Warning Intelligence Services (3.3). The contractor shall work on-site at ERDC and AFRL. Personnel located at HPCMPO is optional.
(4) Protect Services (3.4). The contractor shall work on-site at ERDC, AFRL, and HPCMPO.
(5) Infrastructure Services (3.5). The contractor shall work on-site at ERDC and AFRL.
(6) Boundary Assessment and Analysis Services (3.6). The contractor shall work on-site at ERDC, AFRL, HPCMPO, or remotely from any U.S.-based location.
(7) Sustainment Services (3.7). The contractor shall work on-site at ERDC, AFRL, HPCMPO, or remotely from any U.S.-based location.

The contractor may propose to perform Boundary Assessment and Analysis Services (3.6) and/or Sustainment Services (3.7) remotely with positions geographically dispersed, but the Government will not provide a high-speed internet connection or telephone to enable remote support.

Alternate Performance Locations: As directed and approved by the Government, alternate performance locations may be required during the life of this contract. Alternate performance locations may include Government operated and contractor operated locations. Situational teleworking is permissible with prior concurrence from the Government.

2.6.2 Hours of Operation

The contractor shall work during the designated hours of operations for each primary place of performance (ERDC, AFRL, and HPCMPO). Except for services that have been identified as mission essential in accordance with DFARS 252.237-7023, the contactor shall be excluded from working during base closures due to Federal holidays, Government shutdown, weather, or other situations identified by the PCO. Any additional Presidential declared holiday (not one of the standard eleven Federal holidays) or otherwise declared down day will not be a recognized holiday for the contractor.

Tasks requiring 24/7/365 support (e.g., Detect Services) will not be exempt in the event of facility closure and will be considered essential personnel. Personnel will be provided government furnished equipment (GFE) laptops for check-out for proper coverage of tasks in the event of closure. Unclassified work may be accomplished via telework; however classified work must be shifted to alternate CSSP locations identified in Table 1: Maximum Seating Capacity. The contractor shall propose a solution for the coverage of tasks in this event.

a. **Program Manager (3.1).** The core hours are between 7:00 AM and 5:30 PM, Monday through Friday, local time. The contractor shall provide on-call support during non-core hours, which may require them to work additional hours outside of the core hours.
b. **Detect Services (3.2)**. Performance is on a 24/7/365 basis and are considered mission-essential functions.
c. **Warning Intelligence Services (3.3)**. The core hours are between 7:00 AM and 5:30 PM, Monday through Friday, local time. The contractor shall provide on-call support during non-core hours, which may require them to work additional hours outside of the core hours.
d. **Protect Services (3.4)**. The core hours are between 7:00 AM and 5:30 PM, Monday through Friday, local time. The contractor shall provide on-call support during non-core hours, which may require them to work additional hours outside of the core hours.
e. **Infrastructure Services (3.5)**. The core hours are between 7:00 AM and 5:30 PM, Monday through Friday, local time. The contractor shall provide on-call support during non-core hours, which may require them to work additional hours outside of the core hours.
f. **Boundary Assessment and Analysis Services (3.6)**. The core hours are between 7:00 AM and 5:30 PM, Monday through Friday, local time. The contractor shall provide on-call support during non-core hours, which may require them to work additional hours outside of the core hours.
g. **Sustainment Services (3.7**). The core hours are between 7:00 AM and 5:30 PM, Monday through Friday, local time.

The contractor may be required to work additional hours outside of the core hours for Boundary Assessment and Analysis Services, Infrastructure Services, Warning Intelligence Services, Program Manager, and Protect Services as part of the standard (i.e., not Surge) services.

The contractor shall have the capability and capacity to provide surge labor and acquisitions in response to a government directed action as directed in Section 2.15.

2.7 Federal Holidays

Except for the services that are required 24/7/365, the contractor shall not provide services on the following recognized federal holidays without prior authorization from the PCO:

- January 1, New Year's Day
- 3rd Monday in January, Martin Luther King Jr. Holiday

- 3rd Monday in February, Presidents Day
- Last Monday in May, Memorial Day
- June 19, Juneteenth National Independence Day
- July 4, Independence Day
- 1st Monday in September, Labor Day
- 2nd Monday in October, Columbus Day
- November 11, Veterans Day
- 4th Thursday in November, Thanksgiving Day
- December 25, Christmas Day
- Any other day designated by Federal statute, executive order, or presidential proclamation.

When a holiday falls on a Sunday, it is observed on the following Monday, or as by directed by the official US Office of Personnel Management Federal Holiday Schedule. When a holiday falls on a Saturday, it is observed on the previous Friday, or as by directed by the official US Office of Personnel Management Federal Holiday Schedule.

2.8 Government Facility Closure

In the event of a Government facility closure, the contractor employees shall be excused from work at no cost to the government. The contractor shall continuously provide the services that are required 24/7/365.

There may be local determinations relating to adverse weather conditions, national emergencies, energy conservation, executive order determinations, furloughs, etc., which may require one or more facilities to close or reduce facility access. Since there is 24/7 coverage required for this contract, work may be required at the respective facilities to be determined by the local authority.

2.9 Citizenship

Contractor and employees of the contractor are required to be citizens of the United States of America and must maintain such status during the entire duration of the contract.

2.10 Security Clearances

The highest level of clearance required for this order is TOP SECRET (TS) clearance with Sensitive Compartmented Information (SCI). For minimum requirements, refer to Table 2: Minimum Clearance Requirements:

Table 2: Minimum Clearance Requirements

Requirement	**Minimum Clearance**
Boundary Assessment and Analysis Services	SECRET; privileged access on classified systems requires a favorable Tier 5 (T5) background investigation
Warning Intelligence Services	TOP SECRET / SCI with T5 investigation
Protect Services	SECRET; personnel supporting Insider Threat (3.4.7) require TOP SECRET / SCI; privileged access on classified systems requires a favorable Tier 5 background investigation
Detect Services	SECRET; privileged access on classified systems requires a favorable Tier 5 background investigation
Sustainment Services	SECRET; privileged access on classified systems requires a favorable Tier 5 background investigation
Infrastructure Services	SECRET; privileged access on classified systems requires a favorable Tier 5 background investigation

The Contractor shall perform all TS/SCI functions required on this contract at approved Government locations. The contractor shall provide security at a level necessary to meet the requirements of the tasks requested. The contractor will require access to the Secret Internet Protocol Router Network (SIPRNET), SECRET DREN (SDREN), and the applicable Security Classification Guides (SCGs). SIPRNET/SDREN accounts will be requested through the Government and access to SIPRNET/SDREN will be at Government locations only. The contractor will require access to For Official Use Only and other Controlled Unclassified Information (CUI).

The contractor shall meet the requirements of the contract DD Form 254. The solicitation incorporates a DRAFT DD Form 254. The final, signed DD Form 254, will be incorporated into the order upon award or via modification.

The Contractor shall possess a TOP SECRET facility security clearance. Any proposed subcontractor that will execute any secured portion of this contract must also be included on line 7 of the DD254 and must possess the applicable security clearance level to the work that they will execute under this contract. The Government assumes costs and conducts security investigations for security clearances. The contractor shall request security clearances for personnel requiring access to classified information within 15 calendar days after service award. Due to costs involved with security investigations, requests for contractor security clearances shall be kept to an absolute minimum necessary to perform service requirements. The contractor shall submit a Visit Request to the appropriate security office before arriving at a Government facility. The contractor shall retrieve all identification media, including vehicle decals, from employees who depart for any reason before the contract expires; e.g., terminated for cause, retirement.

2.11 Common Access Card (CAC)

Each contract employee will be issued a CAC by the Government. The CAC shall be returned by the contract employee to the issuing office upon termination of employment, reassigned outside of this contract, or at the expiration of this contract. Each contract employee shall wear the CAC such that it is readily visible at all times during contract performance at official duty station. The CAC shall not be displayed while away from the official duty station or be left visible in a vehicle.

2.11.1 Contractors who do not require 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 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, as NCIC and TSDB are available), or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations.

2.12 Travel

The Government may require the contractor to travel to military and non-military locations in support of these requirements. Some travel may support crisis actions/operations. Travel must be approved by the COR and/or PCO and a modification to the contract issued before a trip is begun. If prior Government approval is not obtained, the contractor shall not be reimbursed. The contractor will not be reimbursed for travel in their local area.

2.12.1 Travel Approval

A contractor-generated travel authorization request form shall be submitted to the COR and/or PCO for approval prior to beginning any travel. The travel request shall, at a minimum, include:

- Traveler(s) name(s)
- Travel dates, inclusive
- Travel location(s)
- Purpose of trip
- Itemized list of expenses to include lodging, lodging tax, meals and incidental expenses (per diem), transportation costs, tolls, parking, and any other allowable expenses in accordance with FAR 31.205-46.
- Proof of Airfare cost, if applicable
- Proof of Rental car cost, if applicable
- Other information as required by the COR and/or PCO.

All travel requests must be submitted to the COR and/or PCO fifteen (15) calendar days prior to the date of travel, if the need to travel is known and anticipated. Regardless, the contractor shall submit requests with sufficient time for Government review and approval. The PCO will review the contractor request and upon approval, the PCO will execute a modification to the contract for the contractor travel event.

2.12.2 Travel Reimbursement

Travel costs will be reimbursed according to the modification amount agreed to by the contractor and the Government. Travel costs will be set at the allowable rates and in accordance with FAR 31.205-46. Profit shall not be applied to nor allowed on travel costs. Travel shall be in compliance with the contract tasks and all other applicable requirements, and maximum use is to be made of the lowest available customary standard coach or equivalent airfare accommodations available during normal business hours. The Government is not liable for any travel costs that were not pre-approved on the agreed to modification. Minimal overage of costs on prior approved expenses will be paid on a case by case basis. Any overage that is known or realized by the contractor employee shall be immediately communicated to the COR and/or PCO to ensure adequate funding is available for reimbursement. Any increase in costs due to additional temporary duty days (only at the request or direction of the Government) will require prior authorization and further modification. Contractor shall submit all receipts for travel to substantiate their travel reimbursement request.

2.12.3 Trip Reports

The contractor shall deliver a trip report no later than five (5) business days after completion of travel. A trip report shall include the traveler(s) name(s), travel date(s), travel location(s), reason for travel, actions items resolved during travel, and actions still pending resolution. The contractor shall submit the trip report to the COR and PCO and provide a copy of the report with its travel reimbursement request. Contractor format is acceptable.

2.13 Training

The Government may require the contractor to attend courses to acquire knowledge of hardware or software added to Government DoD networks. If travel is involved, that must be approved separately in accordance with PWS 2. "Travel." Training must be approved by the COR and/or PCO before a course is begun. If prior Government approval is not obtained, the contractor shall not be reimbursed. The contractor will not be reimbursed for formal educational training or general commercial hardware/software system training, or to meet the requirements of 4.1.11.

2.13.1 Training Approval

A contractor-generated training authorization request form shall be submitted to the COR and/or PCO for approval prior to beginning any course. The contractor shall ensure that the requested training costs will not exceed the amount authorized in this order. The training request shall, at a minimum, include:

- Employee(s) name(s)
- Course dates, inclusive
- Course description
- Purpose of training
- Expenses for course registration
- Other information as required by the COR and/or PCO. The COR is authorized to approve training requests.

All training requests must be submitted to the COR and/or PCO thirty (30) calendar days prior to the date the course is scheduled to begin. The PCO will review the contractor request and upon approval, the PCO will execute a firm fixed price modification to the contract for the contractor training event.

2.13.2 Training Reimbursements

Training costs will be reimbursed according to the firm fixed price modification amount agreed to by the contractor and the Government. The Government is not liable for any training costs that were not pre-approved or exceed the funded ceiling amount of the negotiated modification to the contract for the contractor training event. Proof of completion of the training will be required to be submitted with the training reimbursement request.

2.14 Key Personnel

Key personnel are deemed critical to successful performance of the requirements. Any position identified as key shall remain so for the duration of this task order.

The contractor shall, for the term of this task order, not make key personnel substitutions or additions unless necessitated by compelling reasons including, but not limited to: an individual's illness, death, termination of employment, declining an offer of employment (for those individuals proposed as contingent hires), family friendly leave, or unavailability for any other reason. In such an event, prior to the substitution or addition of key personnel, the contractor shall submit a request of approval to the COR in writing, with approval coming from the PCO. All proposed substitutes (no matter when they are proposed during the performance period) shall have qualifications that are equal to or higher than the qualifications of the person being replaced.

If the PCO determines that suitable and timely replacement of key personnel who have been reassigned, terminated, or have otherwise become unavailable to perform under this task order is not reasonably forthcoming or that the resultant reduction of productive effort would impair the successful performance of the contract requirements, the contract may be terminated by the PCO for default or for the convenience of the Government, as appropriate.

Key Personnel and the related requirements of each are identified in the following subsections:

2.14.1 Program Manager

- Possess at least a Bachelor's degree in computer science, information systems, cybersecurity, or other related discipline
- Shall have 10 years IT or cybersecurity related experience
- Shall have at least 5 years of program/project manager experience

2.14.2 Lead Detect Analyst(s)

- Shall have at least 5 years intrusion detection experience
- Shall be DoD 8570 compliant with CSSP-A or CSSP-IR requirements
- Shall have additional experience in security or network technology (Unix/Windows OS, Cisco/Juniper routing/switching) within a hands-on implementation or administration role
- Shall demonstrate thorough knowledge of Transmission Control Protocol/Internet Protocol (TCP/IP) protocol implementations for all common network services in addition to demonstrated capability to perform network packet analysis and anomaly detection

2.14.3 Detect Shift Leads

- Shall have at least 5 years experience handling cyber and security incidents (NIST SP 800-641)
- Shall have experience correlating cyber defense trends and reporting
- Shall be DoD 8570 compliant with CSSP-A or CSSP-IR requirements
- Shall have additional experience in security or network technology (Unix/Windows OS, Cisco/Juniper routing/switching) within a hands-on implementation or administration role
- Shall demonstrate thorough knowledge of TCP/IP protocol implementations for all common network services in addition to demonstrated capability to perform network packet analysis and anomaly detection

2.14.4 Lead Protect Analyst

- Shall have at least 5 years ISCM, insider threat, and/or protect services (e.g., Endpoint System Security (ESS), Assured Compliance Assessment Solution (ACAS), Automated Continuous Endpoint Monitoring (ACEM)) experience
- Shall be DoD 8570 compliant with CSSP-A or CSSP-IR requirements
- Shall have additional experience in Windows and/or Linux management and support within a hands-on implementation or administration role
- Shall demonstrate thorough knowledge of TCP/IP protocol implementations for all common network services in addition to demonstrated capability to perform network packet analysis and anomaly detection

2.14.5 Lead Systems Engineer

- Shall have at least 5 years Network and Systems Engineering experience
- Shall be DoD 8570 compliant with CSSP-IS requirements
- Shall have additional experience in Windows and/or Linux management and support within a hands-on implementation or administration role

- Shall demonstrate thorough knowledge of TCP/IP protocol implementations for all common network services in addition to demonstrated capability to perform network packet analysis and anomaly detection

2.15 Surge

Surge is additional effort that is required to support these requirements due to events that are short-notice, emerging, or rapidly changing. This is typically planned, but may be unplanned to provide a higher level of support during some periods of time. Surge will be separately priced from the baseline requirements of this PWS.

2.15.1 Surge Approval

Surge must be approved by the COR and/or PCO before performance is begun, even if the event is unplanned. The Government will not pay for any surge work that is performed without prior approval or initiated by the Government.

Upon request by the Government, the Contractor shall submit a proposal to the COR and/or PCO detailing the level of effort and costs needed to support the surge event requirements of the Government. These surge requirements can either be planned or unplanned, as identified by the Government. Utilizing the firm fixed price surge labor rates of the contract, the PCO will review, negotiate and approve the contractor submitted proposal and execute a firm fixed price contract modification for the surge event. The contractor shall ensure that the approvedsurge costs will not exceed the amount of funding available on the firm fixed price modification. Only additional surge requirements initiated by the Government shall warrant a further increase to the overall cost of the surge event. In that case, the PCO will initiate a further firm fixed price modification for those additional requirements.

Contractor format is acceptable, but a surge proposal shall, at a minimum, include:

- Date of proposal
- Overview of PWS/Surge Requirements
- Employee name(s)
- Labor category(ies)
- Pre-negotiated surge labor rate(s) (Firm Fixed Price Contract Labor Rates)
- Number of surge labor hours
- Total cost of labor for each employee and total overall cost
- Estimated date/time period for the surge support
- Other information as required by the COR

2.15.2 Surge Reimbursement

The contractor shall prepare a cost breakdown of the surge performed during a billing period, to be submitted with their invoice, which shall include:

- Service period dates (from/to)
- Associated approved surge authorization (Contract Modification Number)
  Charges – broken out by duty title(s), labor category(ies), employee name(s), approved hourly labor rate(s), and hours worked

3 Scope of Work

3.1 Program Manager

The Program Manager shall:

- Be onsite during core working hours (Situational telework must be approved by the Government). For non-core hours, the Program Manager shall respond to the Government within thirty (30) minutes of being contacted by the Government.
- Serve as the primary POC for the contract to the Government
- Collect project data in support of HPCMP CSSP reporting, orders, and tasks
- Apply their management skills and specialized functional and technical expertise to guide project teams in delivering CSSP solutions and assist in managing the day-to-day operations.

- Monitor quality across teams
- Establish and maintain technical and financial reports to show progress of task activities to the Government, organizes and assigns responsibilities to subordinates, and oversees the assigned tasks
- Plan project resources by developing shift schedules, monitoring analyst and staff workloads, and ensuring that performance aligns to the Government's goals and objectives for providing CSSP services
- Ensure that responsibilities and workloads are properly and evenly distributed throughout all CSSP locations to ensure shared understanding and load amongst the team
- Ensure that all personnel are appropriately trained and cleared to their respective position.
- Communicate any resource constraints, as well as staffing levels and issues with workload to the Government regularly, timely, and formally through the monthly report
- Be intimately aware of all personnel's job duties and expectations
- Proactively communicate any foreseen issues in performance, scheduling, and any needed changes in processes or training
- Provide operational and logistical services, as well as recommend updates to project information. This includes participation in project reviews, and the development of formal presentations and information papers
- Support the quarterly CSSP Quality Assurance (QA) process and Weekly Director's Update Briefing by providing metrics in support of CSSP performance
- Prepare presentations, reports, and maximizing schedule efficiencies based on information provided about subscriber systems to be evaluated to include system specifications and appropriate skill sets
- Be responsible for preparing and coordinating for DoD evaluation and inspection activities, including taking steps to ensure all gaps are addressed in a timely manner prior to and after the evaluation or inspection activity.
- Ensure that all key performance indicator (KPI) targets are being achieved through the QA process
- Coordinate the gathering of periodic status reports/communications to stakeholders on major incidents, other priority incidents and issues through the bimonthly subscriber briefing and other ad hoc report requests
- Provide weekly communication to management on issues, risks, accomplishments, MOA breaches, and KPIs
- Communicate status updates to executive leadership
- Continuously identify, document, and present opportunities of improvements to the Government
- Implement best practices and approved improvements
- **(AM #0005)** Possess no less than a secret clearance. (**AM #0005)**

3.1.1 Personnel Management

Personnel performing cybersecurity functions must be properly trained and equipped in order to maximize effectiveness. The staff must also be sufficiently manned to effectively provide services to their subscribers.

The contractor shall:

- Assist the organization in monitoring training and staffing requirements of Government and Contractor employees to remain fully capable
- With the input and approval of the Government, develop and maintain a documented workforce plan, including both Government and Contractor employees, to include: documented position descriptions for all staff, level of effort, listing of functional roles and responsibilities, required security clearance, investigative, and access requirements, system privilege level requirements, training and certification requirements
- Update the formal workforce plan annually and as needed to sustain current operations
- Verify staff have completed formal screening, are fully qualified IAW DoD Guidance, and are cleared to the appropriate security clearance level as identified in the formal Workforce Plan
- With the input and approval of the Government, develop and maintain a formal training program for the Contractor
- Document and maintain all training records (e.g., class roster, database (DB), training records, etc.) related to for all staff. Training program should ensure include requirements IAW DoD 8570/8140 and any other training required by organization. Training program should include all software/hardware cybersecurity

tools, products, and organizational cybersecurity Standard Operating Procedures/ Techniques, Tactics, Procedures (SOPs/TTPs) required for use by staff

3.1.2 On-Call Support
The contractor shall provide on-call support during non-core hours.

Support shall consist of normal duties during non-core hours in the event of a cybersecurity event, named operation, or other activity requiring urgent actions.

3.2 Detect Services

Detect services include attack sensing and warning (AS&W) and cyber incident handling. Detect is the collection, normalization, correlation, and characterization of event and incident data to identify anomalous or unauthorized activity, including cyber intrusions, attacks, data loss, or other prohibited activities (pornography, gambling, etc.) coupled with the notification to command and control, following established guidance for response, and coordinating or escalating with subscribers and higher command. This data comes from all available sources including but not limited to: sensor logs and data, device logs, security application logs, Host Based Security System (HBSS) data, incident tickets, archives, etc. The contractor shall perform this requirement continually on a 24/7/365 basis.

The contractor shall consider the paradigm shift of performing these services for DODIN on premise assets, as well as, DODIN assets that reside in commercial cloud instances. The contractor shall utilize on premise, Government-provided Defensive Cyber Operations (DCO) capabilities, as well as cloud-native DCO capabilities within the cloud. The CSSP service is designed to protect against, defend, and respond to suspicious or malicious cyber activity associated with network traffic entering or exiting the HPCMP Virtual Private Cloud (VPC) Secure Cloud Computing architecture (SCCA).

Review Time: Critical and high alerts shall be reviewed within fifteen (15) minutes of entering the security information and event management (SIEM) tool. Medium alerts shall be reviewed within forty-five (45) minutes of entering the SIEM. Low alerts shall be reviewed within one (1) hour of entering the SIEM. The contractor shall review 95% of alerts within their associated timelines.

Response Time: Critical and high alerts shall be reviewed and adjudicated within thirty (30) minutes of entering the SIEM. Medium alerts shall be reviewed and adjudicated within ninety (90) minutes of entering the SIEM and low alerts shall be reviewed and adjudicated within twelve (12) hours of entering the SIEM.

In support of these activities, the contractor shall:

- Review/analyze the correlated data from the provided Security Event and Incident Management (SEIM) system. This data comes from a variety of sources (host logs, host based security logs, vulnerability data, network intrusion detection logs, web content filtering, web application firewalls, firewalls, network devices, DNS logs, file hashes, behavioral analytics, indicators of compromise (IOCs), etc.);
- Use correlated data analysis to identify unauthorized activity, evaluate the likelihood of success of the activity based on available information (utilizing ISCM data and knowledge of attack/vulnerability targets), and create incident response tickets for investigation by Incident Responders within reporting timelines outlined in CJCSM 6510.01B;
- Ensure that reports are peer-reviewed and less than 10% of reports are rejected due to error.
- Utilize the Unified Kill Chain model during incident analysis activities to recommend appropriate countermeasures (Detect, Deny, Disrupt, Deceive, etc.) across all layers of the defense-in-depth model to effect all phases of the attack;
- Report all appropriate incidents and events to JIMS or other designated platform within required timelines based on CJCSM 6510.01B requirements;
- Pass the Joint Qualification Requirement (JQR) test and onboarding process within 90 days of assignment;
- Follow Joint Force Headquarters – Department of Defense Information Network (JFHQ-DODIN) guidelines for reporting significant activity (SIGACT), or issuing notifications (e.g., ‘TIPPERs’) to other CSSPs or Area of Operation Commander/Directors when activity is detected;

- Monitor for effectiveness of identified countermeasures, a process generally referred to as Active Cyber Defense Cycle;
- Provide Incident Response, evaluating the efficacy of containment and eradication of intrusions;
- Summarize and categorize security events (notifications, attacks, Trojans, command and control, exploits, etc.) for all DREN/SDREN by subscriber, notifying increases in activity/categories for DREN/SDREN or individual subscribers;
- Monitor log collection/pipeline processing from all sources of sensors/correlated data and immediately notify CSSP Infrastructure when reporting has not occurred in more than 2 hours and has not been previously reported as an outage;
- Identify gaps in coverage or visibility necessary to identify if a possible intrusion has occurred and recommend corrective action to the Government.
- Follow procedures that are IAW NIST SP 800-61 and DOD M-6510.01 Volume I/CJCSM 6510.01B, for the handling of incidents
- Collect intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
- Report incidents and events within proper channels and within timelines identified in the CJCSM 6510.01B
- Identify, document, and report unauthorized activity/attacks (including IP addresses and ports, attack vector, and attack timeframe) in all incidents and reports per HPCMP CSSP SOPs
- Take action, if appropriate, to prevent or mitigate potential impact to the DODIN based on cyber threats, and develop and distribute countermeasures and interim guidance to prevent or mitigate threats and/or attacks on DODIN
- Monitor a platform capable of performing information security continuous monitoring (ISCM) for the purposes of detecting cyber intrusions, attacks, anomalous behavior, and possible insider threats.
- Provide a 24/7/365 event/incident handling and analysis capability
- Provide detailed information regarding the event IAW CJCSM 6510.01B
- Provide operations log accessible to personnel documenting all mandated reportable cyber events/incidents
- Analyze detected cyber events to identify incidents
- Categorize and characterize cyber incidents
- Ensure JFHQ-DoDIN and other DOD CSSPs have visibility and insight into detected cyber incidents and cyber incident response actions complete with Course of Action and implementation via the Joint Incident Management System (JIMS), SIGACTs, and tippers
- Ensure proper reporting of incidents requiring Security, Law Enforcement and/or Counter Intelligence (LE/CI) involvement
- Notify affected Subscribers of cyber incidents and collect assessments of mission impact for the loss of the system during the incident response process
- Provide initial response to cyber incidents per HPCMP CSSP SOPs
- Take initial steps to contain cyber incidents
- Ensure forensically sound acquisition and preservation of incident data
- Support Subscriber’s actions in incident response by assisting with cyber component reporting, coordinating countermeasure deployment, and maintaining the subscriber personnel escalation process and up-to-date rosters
- Analyze cyber incidents to develop specific responses
- Develop and implement comprehensive cyber incident process
- Distribute tailored countermeasures or interim guidance to Subscribers to eradicate and prevent cyber incidents across all subscribers
- Perform forensic analysis of systems and malware in cases where subscribers lack the capability and ensure relevant IOCs are shared with Warning Intelligence
- Mitigate operational and/or technical impact due to cyber incidents
- Contain the spread of malware to prevent further damage to IT systems through detection, analysis, and execution of containment measures
- Work to remove incident root causes through data preservation and guiding subscribers in system rebuilds/system functionality restoration
- Assist Subscribers with cyber incident mitigation efforts

- Manage subscriber accounts in Incident Response Tracker (IRT) to include new accounts, modification, and deactivations
- Assist with research and data validation in support of the battle station reporting requirements
- Prepare documentation and coordinate activities associated with DoD evaluation and inspection activities.

Based on historical data, the Government anticipates the following activities within a given work week, with a variation of +/- 10%.

- Alert Volume: 4 critical / 3,000 high / 52,000 medium / 60,000 low
- Incident and Event Reports Filed: 13
- Countermeasures Implemented: 15
- Basic Indicators of Compromise (IPs, domains, etc.) added to SEIM: 1,200
- New Detection Logic (code based detection) added to SIEM: 2

3.2.1 Lead Detect Analyst(s)
The Lead Analyst(s) shall:

- Employ effective web, email, and telephonic communications to clearly manage subscriber related issues; Review and prepare trend analysis, metrics, and other relevant data for presentation during to be used for briefing leadership, partners, and subscribers regarding computer network defense
- Maintain training and quality assurance program
- Perform quality assurance review on AS&W alert processing, incident reporting, and deliverable.
- Pass the Joint Qualification Requirement (JQR) test and onboarding process within 90 days of assignment.
- Act as a liaison between Government personnel and analysts
- Be responsible for deliverables such as SOPs, AARs, etc.
- Act as an authority for Tier 1 tasks

3.2.2 Detect Shift Leads
The Detect Shift Leads shall:

- Draft incident reports, and review incident reports of other analysts, for quality assurance in accordance with HPCMP SOPs
- Track the status of all open incidents to ensure timely closure in accordance with CJCSM 6510.01B “Cyber Incident Handling Program”
- Distribute computer network defense (CND) alerts among personnel performing tasks 3.2
- Serves as a subject matter expert in the analysis of alerts
- Employ effective web, email, and telephonic communications to clearly manage security incident response procedures
- Consolidate trending of cyber incidents and create the products that are required to be used for briefing leadership, partners, and subscribers regarding computer network defense
- Pass the Joint Qualification Requirement (JQR) test and onboarding process within 90 days of assignment.
- Be onsite 24/7/365 at one (1) location from Table 1: Maximum Seating Capacity unless otherwise directed by the government
- Perform Battle Captain duties during non-core hours. Battle Captain duties include:
    - Review released warnings, orders, notifications, and other products from higher commands
    - Interpret and distribute to appropriate personnel for action within one hour of release per HPCMP CSSP SOPs
    - Employ effective web, email, and telephonic communications to clearly manage the cyber orders process
    - Enact escalation procedures to Government personnel per the HPCMP CSSP Incident Response Plan
    - Share AS&W information, warning intelligence information (notifications, notes, and reports), countermeasures (proposed and tailored), and interim guidance with JFHQ-DoDIN and other DOD CSSP providers
    - Share proposed and tailored countermeasures or interim guidance with JFHQ-DoDIN, other DOD CSSP providers and Subscribers

3.2.3 CSSP Subscriber Response

The contractor shall:

- Provide subscriber support and issue tracking for all subscribers
- Respond to subscribers' support requests within one (1) hour and open a trouble ticket within 90 minutes after 1st contact
- Document and share monthly percentages on the number of total subscriber calls received, tickets created, and issues resolved

3.3 Warning Intelligence Services

Warning Intelligence services support the detection and reporting of time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intentions against U.S. partners or interests. Cybersecurity service providers receive, analyze, and distribute relevant warning intelligence information received from intelligence sources. Cybersecurity service providers contribute by developing and distributing countermeasures or interim guidance to detect, prevent, or mitigate potential cyber event impacts to the DODIN to its subscribers.

In support of these activities, the contractor shall:

- Monitor closed and open-source intelligence daily for early warning intelligence of severe vulnerabilities, zero days, or likely threat actor targeting of organization domains;
- Provide concise, time-relative Situational Awareness Reports (SARs) to operations personnel and organization stakeholders based on daily closed and open-source monitoring activities and generated Warning Intelligence on a recurring basis;
- Provide mitigation recommendations and detection support across multiple layers of the defense-in-depth model;
- Pass the Joint Qualification Requirement (JQR) test and onboarding process within 90 days of assignment.
- Collect, maintain, and fuse data gathered from all intelligence sources (closed, open, internally generated, and commercially provided) on a continuous basis;
- Create, update, and maintain threat models that incorporate knowledge of cyber terrain (mission, critical assets, industry supported, attack surface, network and domain footprint, and attack/intrusion history);
- Use common Warning Intelligence techniques (diamond model, cyber kill chain, and MITRE ATT&CK) to generate and maintain historical tactics, techniques and protocols (TTPs), historical infrastructure, and recent activity for significant threat actors/groups;
- Create and maintain a heat map of active adversarial campaigns against DREN/SDREN relevant terrain to be briefed quarterly to Government management and stakeholders;
- Continually perform cyber hunt activities for threat actors/groups within DREN/SDREN relevant terrain. The contractor shall work closely with Detect personnel to ensure timely reporting and tracking potential incidents;
- Support CSSP operations during serious intrusion events (CAT-1, 2, and 4) to provide insight and attribution of threat actor activity to include attack timelines, attacker tactics, techniques and protocols (TTPs), and fusion of other intelligence sources;
- Provide CSSP operational support for on-site cyber-data forensic collection and chain-of-custody for serious intrusion events (CAT-1, 2, and 4) to include volatile memory collection and drive replication;
- Monitor the incident and event reports generated by Detect personnel in order to apply adversarial attribution.
- Review all intelligence tippers and bulletins, and draft accompanying signatures within twenty-four (24) hours from the time that intelligence is received
- Review all incident reports via Incident Response Tracker (IRT) for attribution to intelligence gathered and correlation of data across incidents
- Receive and take initial action on warning intelligence information received from intelligence organizations
- Perform preliminary analysis on warning intelligence information
- When appropriate, perform forensic investigations and produce a detailed forensics report of findings
- Analyze cybersecurity threats
- Identify potential impact to Subscriber operations through analysis of warning intelligence information

- Analyze intelligence reports, forensic reports, and reverse engineering of malware reports to determine associated indicators of compromise (IOCs) and utilize the IOCs to develop and distributes countermeasures to detect and prevent identified threats to operations across the Kill Chain™
- Collect intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation
- Evaluate IOCs derived from incidents within the CSSP to determine association with known computer network exploitation (CNE) groups and thoroughly investigate the IOCs for other infrastructure possibly related to the CNE teams (domain registrations, IP ownership, VPN infrastructure, strains of malware, etc.) for consideration of additional proactive defensive measures
- Enable Subscribers to prevent or mitigate the potential impact of cyberattacks
- Develop and distribute countermeasure to prevent/mitigate potential cyber event impacts to DODIN
- Coordinate with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents
- Prepare documentation and coordinate activities associated with DoD evaluation and inspection activities.

Based on historical data, the Government anticipates the following activities within a given work week/month, with a variation of +/- 10%.

- Closed-source reports reviewed: 30/week
- Open-source reports reviewed: 100/week
- Internal Warning Intelligence articles/news generated: 1 bi-weekly
- Warning Intelligence Situational Awareness Reports (SARs): 1/week
- Warning Intelligence APT research and reporting: 1/week

3.3.1 CSSP Subscriber Response
The contractor shall:

- Provide subscriber support and issue tracking for all subscribers
- Respond to subscribers' support requests within one (1) hour during core hours and open a trouble ticket within 90 minutes after 1st contact during core hours. Requests during non-core hours may be deferred until the next working day
- Document and share monthly percentages on the number of total subscriber calls received, tickets created, and issues resolved

3.3.2 On-Call Support
The contractor shall provide on-call support during non-core hours.

Support shall consist of normal duties during non-core hours in the event of a cybersecurity event, named operation, or other activity requiring urgent actions.

3.4 Protect Services

Protect services support the ability to limit or contain the impact of a potential cybersecurity event. As described in DODI 8530.1, Enclosure 3 and CJCSM 6510.01 Enclosure A, CSSP Protect services are categorized into the following areas:

- Vulnerability Assessment and Analysis
- Vulnerability Management
- Endpoint Protection
- Cybersecurity Protection Condition
- Information Security Continuous Monitoring
- Insider Threat

Based on historical data, the Government anticipates the following activities within a given work week, with a variation of +/- 10%.

- Information Assurance Vulnerability Management (IAVM) Notices: 10

3.4.1 Lead Protect Analyst

The Lead Protect Analyst shall:

- Review and track subscriber support issues and tickets and ensure timely follow-up and resolutions
- Engage infrastructure team for troubleshooting systems that impact team resolution
- Ensure all configuration changes and system updates are properly vetted and aligned with configuration management requirements established by the Government
- Serve as a subject matter expert in the analysis and administration of vulnerability scans and/or HBSS configuration, operation, and management
- Employ effective web, email, and telephonic communications to clearly manage subscriber related issues; Review and prepare trend analysis, metrics, and other relevant data for presentation during to be used for briefing leadership, partners, and subscribers regarding computer network defense
- Pass the Joint Qualification Requirement (JQR) test and onboarding process within 90 days of assignment.
- Prepare documentation and coordinate activities associated with DoD evaluation and inspection activities.

3.4.2 Vulnerability Assessment and Analysis

The contractor shall ensure the deployment and availability of DoD's ACAS system which is configured in accordance with DISA ACAS best practice guides for performing compliance scans on both DREN and SDREN, and that the system is able to accept vulnerability data from subscribers who deploy ACAS scanners locally onsite.

Additionally, the contractor shall ensure that:

- Subscribers and CSSP use DoD approved tools (ACAS) to conduct vulnerability assessments;
- Processes are developed for communications with subscribers who fail to meet minimum standards, striving for remediation within one (1) week of failed scans, and that remediation of vulnerabilities is achieved within defined DoD timelines (e.g., 21 days for Information Assurance Vulnerability Management (IAVM) notices). The contractor shall acknowledge subscriber requests for assistance within one (1) business day and provide daily subscriber updates, unless otherwise directed by the Government;
- Open and unauthorized Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports in accordance with DODI 8551.1 and based on the Category Assurance List (CAL) are identified monthly;
- A formal vulnerability assessment and analysis improvement process is established for capturing lessons learned from the analysis of mitigation actions into the Joint Lessons Learned Information System (JLLIS) and for implementing corrective actions based on the lessons learned.
- Use DoD-approved and recommended tools to conduct vulnerability assessments to evaluate the ability of or compliance with DREN/SDREN defense plans and DODIN operations' activities
- At a minimum, once a week and in accordance with CJCSI 6510.01F and CJCSM 6510.02 and all JFHQ-DoDIN vulnerability scanning orders:
    a. Conduct vulnerability scans IAW JFHQ-DoDIN guidance (e.g., frequency, method, capability). 95% of all scans performed shall be properly credentialed scans. If unable to attain a 95% credentialed scan rate, contractor shall provide justification and remediation actions taken within 1 week of failed scans. Nessus Agents and Nessus Network Monitor (NNM) should be deployed as directed by JFHQ-DoDIN
    b. Identify open and unauthorized Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports IAW DODI 8551.1 and based on the Category Assurance List (CAL)
    c. Identify misconfigurations and vulnerabilities in operating systems, applications, services, and any other software
    d. Take appropriate action to correct findings in a prioritized manner and validate effectiveness of executed actions. Priority should be given to exploitable vulnerabilities that could negatively impact mission success should they be successfully exploited
    e. Maintain status of vulnerability remediation in a POA&M
- Provide JFHQ-DoDIN visibility and insight into the DREN/SDREN to assess risk to the DODIN through reports, findings, and analyses resulting from vulnerability assessments

- For subscriber sites/enclaves, analyze network and host vulnerability scan results and provide copies of results and recommendations to JFHQ-DoDIN monthly
- Perform automated reporting of network and host scan results, as required, IAW supporting DoD guidance and directives
- For all DREN/SDREN enclaves (including non- subscriber enclaves), collaborate with enclaves and their CSSPs to ingest vulnerability scan data
- Establish a formal vulnerability assessment and analysis improvement process by capturing lessons learned from the analysis of mitigation actions from vulnerability and intrusion assessments, exercises, and DOD cyber red team operations
- Prepare documentation and coordinate activities associated with DoD evaluation and inspection activities.
- Pass the Joint Qualification Requirement (JQR) test and onboarding process within 90 days of assignment.

3.4.3 Vulnerability Management

In support of these activities, the contractor shall:

- Establish processes to effectively manage the vulnerability program;
- Obtain, update, and maintain an inventory of all hardware, operating systems, and applications, minimally including contractor, version, and major system components. The Government will provide the tools to record and update inventories. The contractor shall build processes around those tools to analyze those inventories, address any issues, and ensure that they meet the requirements of CJCSM 6510;
- Monitor for IAVA alerts and bulletins, distribute them within 24 hours of issuance to all subscribers, monitor subscriber response and acknowledge receipt (within 1 week) to 95% of notifications, and communicate with delinquent subscribers to ensure receipt. Monitor and track subscriber compliance with IAVA alerts and compliance deadlines, and request Plan of Action and Milestones (POA&M) for each vulnerability not corrected by established deadlines for each subscriber.
- Perform trend analysis quarterly on scan results to identify vulnerability trends that could negatively impact the DREN/SDREN assets and capabilities, including the highlighting of significant non-compliance of subscribers. Analysis should include, at a minimum: increase/decrease in number of vulnerabilities, trends in detected vulnerability severity or category, recurring vulnerabilities, common vulnerabilities among networks are identified and protections are implemented, and identification of global vulnerability trends that could negatively impact mission.
- Use DOD-approved tools for enterprise management, technology driven system inventory including hardware equipment, operating systems, software applications, and user authorities that applies DOD required and internally accepted standard security configurations
- Perform hardware/software inventory updates monthly
- Work with Infrastructure team to baseline and maintain assets IAW applicable security technical implementation guides (STIGs) and internally accepted standard security configurations by performing monthly scans and sharing results and plan for remediation with Infrastructure team
- Provide the capability to receive open source, official, and classified threat, vulnerability, and attack notifications; and provide subscriber sites details to take directed corrective actions to mitigate potential vulnerabilities or threats to their assets and capabilities
- Maintain a capability to identify and respond to cyber vulnerability notifications
- Ensure receipt of and comply with JFHQ-DoDIN orders and alerts. Report vulnerability management compliance to JFHQ-DoDIN
- Maintain subscriber accounts in ACAS to include new accounts, modifications, and deactivations
- Prepare documentation and coordinate activities associated with DoD evaluation and inspection activities.
- Pass the Joint Qualification Requirement (JQR) test and onboarding process within 90 days of assignment.

3.4.4 Endpoint Protection

The contractor shall ensure proper implementation and maintenance of DoD mandated and approved enterprise end point protection. The contractor shall monitor DoD policy and provide recommendations to the Government for the proper mix of solutions for HPCMP and its subscriber sites based on applicable technology within those enclaves. The Government will define the deployed solutions based on recommendation, but the contractor shall be responsible for ensuring compliance with all DoD-applicable regulations and orders related to endpoint security through the configuration of those solutions. Possible solutions include:

- Determining the proper configuration of operating system security functions;
- Using the Endpoint Security Solution (ESS) to detect and counter, in real-time, against known cyber-threats to the Department of Defense (DoD) Enterprise. Ensure ESS is configured in accordance with security technical implementation guidelines (STIGs), best practices, and orders including USCYBERCOM TASKORD 16-0080 and related fragmentary orders (FRAGOs);
- Fully deploy ESS (or DoD recommended/authorized tools) to prevent malware incidents
- Automated Continuous Endpoint Monitoring (ACEM) is an endpoint solution that aids in asset visibility. Configure and deploy this solution in compliance with emerging orders.
- Detect and analyze malware; contain the spread of malware and prevents further damage
- Eradicate the malware from infected hosts; employ mitigating actions to prevent reinfection
- Restore functionality and remove temporary containment measures as described in NIST SP 800-83, Revision 1
- Operate and maintain the ESS server(s) IAW STIG requirements and ensure ESS agents are properly deployed to a minimum of 95% of subscribers' hosts and IAW DoD guidance (unless exempted with Government approval)
- Ensure all required ESS modules are properly deployed, up-to-date, and active on 95% of subscribers' hosts (unless exempted with Government approval) and IAW DoD guidance
- Ensure signature based and heuristic based malware protection capabilities are kept up to date with latest malware signatures and/or properly configured and tuned to protect against malware
- Assist subscribers with deployment, tuning, and configuration of ESS modules and policies, via phone and email communication
- Configure ESS to perform periodic scans IAW current DOD guidance
- Implement the capability to detect and prevent malware incidents by employing malware detection and remediation mechanisms to detect and remove malicious malware
- Actively detect malware by ensuring anti-malware software, engines, and signatures are current
- Coordinate malware scan events to minimize operational or mission impact
- Alert application and system owners of new malware
- Work with subscriber to establish ESS test groups for each site in order to perform module tuning and configuration testing before deployments
- Maintain subscriber accounts in ESS to include new accounts, modifications, and deactivations
- Prepare documentation and coordinate activities associated with DoD evaluation and inspection activities.
- Pass the Joint Qualification Requirement (JQR) test and onboarding process within 90 days of assignment.

3.4.5 Cybersecurity Protection Condition (CPCON)

The contractor shall monitor CPCON changes and orders, track, and report responses to Government leadership, and shall maintain copies of CPCON procedures, and develop local measures to implement and communicate when changing CPCON levels. The contractor shall support the CPCON process for subscribers through reviewing and analyzing Identified subscriber mission critical services, Inventory of subscriber system/network Ports, Protocols, and Services (PPS), and copies of network diagrams.

3.4.6 Information Security Continuous Monitoring (ISCM)

ISCM provides constant observation and analysis of the operational states of systems to provide decision support regarding situational awareness and deviations from expectations. ISCM furnishes observation, assessment, analysis, and diagnosis of organizational cybersecurity posture, cyber hygiene, and cybersecurity operational readiness, as outlined in NIST SP 800-137. The Government will provide a correlation tool to integrate various cyber data sets for analysis.

In support of these activities, the contractor shall:

- Identify gaps in data or capability and continuously work to improve and expand sources of information for the purposes of integrating into ISCM with the goal of increasing the situational awareness of the HPCMP;
- Work with network management personnel to collect and analyze network traffic, fault, performance, and bandwidth information/alerts/data to augment detection of network anomalies and potential unauthorized activity;

- Provide a monthly report to Systems Owners and Administrators regarding the effectiveness of security controls through recommendations for security control implementation and mitigation and/remediation of assessment findings, monitor subscriber response and acknowledge receipt (within 1 week) to 90% of notifications, and communicate with delinquent subscribers to ensure receipt.
- Provide System Owners and Administrators a Security Status Notification based off of agreed upon thresholds for risk or threat exposure;
- Establish and maintain a formal ISCM process improvement program to enhance the performance of asset data collection and analysis, the assessment of security controls, and the identification of network traffic fault;
- Capture asset data, such as ESS, and ACAS data sets, and continuously improve and expand collection of information to maximize visibility into networked information systems
- Through the correlation of asset information with supporting threat and vulnerability data, increase situational awareness to enable protection and defense of the DoD HPCMP
- Through the integration of network-centric data sets, maintain ongoing status of traffic, fault, performance, bandwidth, route, and associated network operations
- Assess changes in security controls employed within or inherited by the system and its' environment of operation
- Through recommendations for security control implementation and mitigation and/remediation of assessment findings, provide a monthly report to Systems Owners and Administrators regarding the effectiveness of security controls
- Provide System Owners and Administrators a Security Status Notification any time the overall risk for falls outside of the established risk baseline by more than 20%
- Employ standards to promote data reuse to enhance visibility of threats and vulnerabilities across the mission areas
- Maintain comprehensive asset visibility, attribution, and description to understand the security disposition of organizational IT, their authorized operating boundary, the 'health' of their associated IT assets, and their continued operational reliability to support human intelligence decision making about assets
- Collaborate with DoD components/ organizations and other Government agencies to actively shape the DoD HPCMP's ISCM Program
- Prepare documentation and coordinate activities associated with DoD evaluation and inspection activities.
- Pass the Joint Qualification Requirement (JQR) test and onboarding process within 90 days of assignment.

3.4.7 Insider Threat

The DoD HPCMP utilizes User Activity Monitoring (UAM) and system auditing capabilities to identify and evaluate anomalous activity and enhance the ability to detect, deter, and mitigate insider threats to classified systems.

In support of these activities, the contractor shall:

- Leverage all sources of data available to them for the purpose of detecting insider threats;
- Identify informational/log source gaps that hinder the detection of insider threats and recommend the creation or acquisition of additional capabilities to address these gaps;
- Establish UAM and auditing processes (i.e., capability to monitor use of IT systems) to identify and evaluate anomalous activity;
- Monitor various data sources to detect inconsistent user activity and evaluate events to identify insider threat activity;
- Ensure formal incident handling processes are followed throughout the lifecycle of any detected insider threat incident, including law enforcement/counterintelligence (LE/CI) involvement in accordance with DODD 5205.16 and CNSSD 504;
- Follow standards for insider threat data preservation and maintenance, including securing the data in accordance with Federal and DoD regulations (e.g. personally identifiable information (PII), Health Information Portability and Accountability Act (HIPAA), law enforcement/counterintelligence (LE/CI)) and preserving user activity monitoring (UAM) chain of custody;
- Work with subscribers, as necessary, regarding insider threat protection measures;
- Establish and maintain a formal insider threat process improvement program to enhance the performance of insider threat identification and audit data collection and chain of custody preservation;

- Collaborate with DoD, Army, and non-DoD organizations to actively shape the DoD HPCMP's Insider Threat Program. Establish a UAM and auditing processes (i.e., capability to monitor use of IT systems) to identify and evaluate anomalous activity
- Establish and maintain an Insider Threat Awareness Training Program, including presentations and other training materials to deliver to the workforce on at least an annual basis
- Support the technical aspects of annual Insider Threat reporting requirements to the DoD HPCMP Authorizing Official (AO)
- Prepare documentation and coordinate activities associated with DoD evaluation and inspection activities.
- Pass the Joint Qualification Requirement (JQR) test and onboarding process within 90 days of assignment.

3.4.8 CSSP Subscriber Response
The contractor shall:

- Provide subscriber support and issue tracking for all subscribers
- Respond to subscribers' support requests within one (1) hour during core hours and open a trouble ticket within 90 minutes after 1st contact. Critical issues, including but not limited to a total loss of access to a subscriber facing application or associated backend server, or a compromise of any kind shall be acknowledged and remediation actions communicated (not necessarily remediation complete) within six (6) hours during either core or non-core hours. Medium/Low issues shall be deferred to core hours only and remediation times communicated to the Government for concurrence
- Document and share monthly percentages on the number of total subscriber calls received, tickets created, and issues resolved

3.4.9 On-Call Support
The contractor shall provide on-call support during non-core hours.

Support shall consist of normal duties during non-core hours in the event of a cybersecurity event, named operation, or other activity requiring urgent actions.

3.5 Infrastructure Services

Resources managed by the contractor include, but are not limited to: desktop workstations, laptop computers, file and application servers, storage appliances or storage area networks (SANs), virtual server/desktop environments, network equipment, and cybersecurity. The contractor shall aid in the design of secure and efficient architectures, as well as securely implementing and maintaining the architectures. Table 3: Infrastructure Technologies provides an approximate scope and type of systems/software/technologies the contractor shall manage to deliver CSSP services. This list is subject to change due to the evolution of technologies and required services to CSSP subscribers.

Table 3: Infrastructure Technologies

Technology	Contractor(s)	OS	Quantity
Routers/Switches	Cisco	Cisco IOS XE/ASA	40
Servers	VMware	Windows Server/RHEL	60
User endpoint systems	Dell	Windows 10	300
SAN	Nimble	Nimble	8
ACAS Scanners	Dell	RHEL	130
Containerization	Docker	N/A	-
Application Administration (user accounts, upgrades, etc.)	Various	N/A	-

Tier 1 Capabilities are the critical capabilities required for baseline operations of HPCMP CSSP. Absence of any of these capabilities gravely degrades the team's ability to perform its primary functions. Refer to Table 4: Infrastructure Response Times for performance requirements on Tier 1 capabilities.

Tier 1 Critical Capabilities:

- Network device connectivity to the DREN and SDREN Service Delivery Point
- Intrusion Detection Capability
- Incident Response Tracker (IRT)
- Domain Controllers

Tier 2 Capabilities are capabilities required for full operations of the HPCMP CSSP. Absence of any of these capabilities degrades the team's ability to perform every function in its ideal state. Refer to Table 4: Infrastructure Response Times for performance requirements on Tier 2 capabilities.

Tier 2 Capabilities:

- Production Endpoint Security Solution(s)
- Vulnerability Scanning and Management Tools
- Customer Support Tracker (CST)
- RADIX (GOTS)
- Subscriber Facing Applications
- Linux Patch Servers

Table 4: Infrastructure Response Times

Priority	Trouble Ticket Opened (Core Hours)	Trouble Ticket Opened (Non-Core Hours)	Remediation Actions Communicated / Ticket Updated (not necessarily remediation complete) (Core Hours)	Remediation Actions Communicated / Ticket Updated (not necessarily remediation complete) (Non-Core Hours)	Examples
1 – Critical	≤ thirty (30) minutes	≤ one (1) hour	≤ one (1) hour of ticket initiation, continuing until resolved	≤ two (2) hours of ticket initiation, continuing until resolved	Problem or issue impacting a significant group of subscribers or any mission critical issue affecting critical systems/assets as defined as Tier 1 and Tier 2
2 – High	≤ one (1) hour	≤ two (2) hours	≤ two (2) hours of ticket initiation, continuing until resolved	≤ four (4) hours of ticket initiation, continuing until resolved	Performance and/or reliability degradation of supported services (however, the services are still operational) as defined as Tier 1 and Tier 2
3 – Medium	≤ one (1) business day	≤ one (1) business day	≤ one (1) business day of ticket initiation, continuing until resolved	≤ one (1) business day of ticket initiation, continuing until resolved	Routine support requests (single user support/impact; non-critical software or hardware error or equipment replacement)
4 – Low	≤ one (1) business day	≤ one (1) business day	≤ two (2) business days of ticket initiation, continuing until resolved	≤ two (2) business days of ticket initiation, continuing until resolved	Work that has been scheduled in advance with the subscriber such as server deployment or general service inquiry
5 – Project	≤ one (1) business day	≤ one (1) business day	Weekly	Weekly	Short or long-term projects that are not the result of an outage or issue such as new equipment installs, refreshes, or changes to infrastructure

Although the frequency, quantity, and nature (e.g., priority, complexity, etc.) of future trouble tickets cannot be predicted due to a wide range of variables, historical ranges for each ticket priority are:

- An average of two (2) Critical or High tickets opened per month
- An average of 25 Medium or Low tickets opened per month

3.5.1 Operations

In support of these activities, the contractor shall:

- Manage, update, and provide comprehensive network diagrams that show all subnets (IP address/mask), VLANs, endpoints (output devices, laptops, servers, desktops, etc.), and network devices in accordance with the Evaluator's Scoring Metrics (ESM);
- Manage and update an inventory of all hardware, operating systems, and applications, minimally including contractor, version, and major system components, in accordance with ESM;
- Install and/or maintain infrastructure services supporting cybersecurity environments such as directory services in support of authentication, networking monitoring services, domain name services, virtual hosting infrastructure, etc. that supports the functionality of cybersecurity operations;
- Serve as the System Administrator (SA) for the operating systems, virtualization infrastructure, and storage solutions supporting critical capabilities for the CSSP. As SA, the contractor shall be responsible for capacity/capability management (sufficient CPU, storage, memory) to ensure adequate application performance, and user account management (both local and active directory);
- Develop interface specifications for use within the enclave environments, and ensure that enclave systems and network designs support the incorporation of DoD-directed vulnerability solutions, e.g. IAVA requirements;
- Setup and ship ACAS scanners within 72 hours of new subscriber notification from CSSP Sustainment, unless the Government deems the local site exempt;
- Manage software and hardware of remote ACAS scanners for all CSSP subscribers.
- Provide systems engineering expertise in the design, integration, operation, and maintenance of cybersecurity infrastructure and capabilities
- Possess the necessary technical skills to lead the overall design, engineering, integration, operation and maintenance of a defense-in-depth strategy for cybersecurity infrastructure employed on the Defense Research and Engineering Network (DREN) in support of the HPCMP CSSP
- Be responsible for interfacing with both cybersecurity operations and project personnel in order to formulate engineering requirements, and seek concurrence in satisfying stated objectives
- Define and employ documented procedures for sustainable, continued operations of enterprise CND capabilities, including centralized vulnerability/patch management processes for all systems
- Support the establishment of infrastructure services supporting cybersecurity environments such as directory services in support of authentication, networking monitoring services, domain name services, virtual hosting infrastructure, etc. that supports the functionality of an environment support cybersecurity research, development, and operations
- Develop interface specifications for use within the enclave environments. Ensure that enclave systems and network designs support the incorporation of DoD-directed vulnerability solutions (e.g. IAVA requirements)
- Utilize defense-in-depth strategies and methods to harden CSSP systems and networks (e.g. blocking/filtering, IDS/IPS, A/V, logical separation of management traffic, content detonation and automated analysis, and DISA SRG/STIG compliance)
- Ensure secure backup of CSSP systems and data through formally documented backup plan, accurate and up-to-date listing of CSSP systems to be backed up, proper storing and labeling of completed backups. In disaster recovery and exercise situations, execute COOP and restore minimum operating capability within three (3) hours regardless of core or non-core hours (intrusion detection sensors, vulnerability scanners and associated servers, endpoint protection tools, Active Directory, VOIP) and within two (2) days, restore operating capability for full suite of CSSP services.
- Manage subscriber account requests for CSSP toolsets utilizing CSSP-managed authentication services
- Prepare documentation and coordinate activities associated with DoD evaluation and inspection activities.

3.5.2 Security
In support of these activities, the contractor shall:

- Define and employ documented procedures for sustainable, continued operations of enterprise DCO-IDM capabilities, including centralized vulnerability/patch management processes for all CSSP systems;
- Maintain a schedule for upcoming software and hardware upgrades and follow procedures for regularly scheduled maintenance and, in the instances necessary, ad hoc, or emergency maintenance. The contractor shall adhere to the HPCMP CSSP Configuration Management Plan for any applicable change made to a system within the CSSP infrastructure. The contractor shall, when appropriate if requested by the COR, participate in the Configuration Control Board as a technical representative to provide information on requested changes to CSSP systems;
- Ensure that all infrastructure is compliant with applicable DoD IAVMs, STIGs, and orders, pertaining to the security posture of the environment. The contractor shall record non-compliance and present that information to the Government for approval in accordance with guidelines identified in the applicable order or instruction. The contractor shall report compliance as needed to the ISSM and assist the ISSM with establishing baseline POA&Ms for non-compliance, as required by DoD 8510;
- Ensure all CSSP systems are no less 90% IAVA compliant with 95% credentialed scans, and 90% STIG compliant unless otherwise agreed upon by Government with all Critical or CAT I findings remediated within one (1) week of discovery;
- Monitor availability and performance of CSSP systems and capabilities with 97% availability for critical capabilities;
- Work with appropriate personnel to ensure IS policies and procedures are documented (e.g., system authorization for all systems supporting CSSP, defense-in-depth measures applied to CSSP systems, anti-malware and system protection are provided to CSSP systems, vulnerability scans and management are addressed, sensitive data transmission is incorporated);
- Ensure all internal networks and information systems are compliant in accordance with DoD Risk Management Framework (RMF) requirements.
- Prepare documentation and coordinate activities associated with DoD evaluation and inspection activities.

3.5.3 Continuity of Operations (COOP)
The contractor shall:

- Ensure business continuity for cybersecurity operations and IT systems. Plans must address emergency, contingency, and/or recovery operations including support for component failures, capability failures, communications failures, personnel availability and site availability are all addressed;
- Ensure secure backup of operational systems and data through a formally documented backup plan, accurate and up-to-date listing of CSSP systems to be backed up, proper storing and labeling of completed backups;
- Execute COOP in disaster recovery and exercise situations, and restore minimum operating capability within three (3) hours regardless of core or non-core hours for Tier 1 services and, within two (2) days, restore operating capability for the full suite of Tier 2 CSSP services;
- Maintain a COOP plan that meets the RMF (NIST SP 800-53 Rev. 4), ESM (Evaluators Scoring Metrics), and CCRI requirements ensuring that the CSSP may maintain business continuity capability while in a COOP configuration. The contractor shall document any COOP activities taken for the purposes of documenting the testing of COOP, as well as lessons learned and after action reviews for review by the Government;
- Test partial COOP of Government-selected critical systems quarterly, and full COOP yearly and submit a report to the Government;
- Recommend the acquisition of new capability or configuration changes to facilitate a complete COOP, if needed, as approved by the Government;
- Coordinate, report (the issue to the service provider if the servicer doesn't acknowledge first), diagnose, and troubleshoot with service providers during VOIP or higher level network outages.

3.5.4 Issue Tracking
- The contractor shall open a trouble ticket for action per the priority requirements defined in Table 4: Infrastructure Response Times when they discover or receive notification of issues related to the

operational infrastructure. Issues shall be acknowledged and remediation actions communicated (not necessarily remediation complete) within the times identified in Table 4: Infrastructure Response Times.

- The contractor shall keep the Government informed as to the progress of all critical issues until final resolution. If equipment replacement is required, the contractor shall notify the equipment contractor and execute return material authorization (RMA) procedures within twenty-four (24) hours of discovery pending funding and equipment availability. Receipt of equipment is subject to contractor delivery times and Government funding availability. Upon receipt of replacement equipment, the contractor shall install and restore service within twenty-four (24) hours. Medium/Low issues shall be deferred to core hours only.
- Project tickets (Priority 5) are defined as a long term project or service requests. Project tickets will be tracked with a minimum of weekly updates. Project tickets will be initiated by Government request. Project scope and timeline will be agreed upon by both the contractor and Government. Project tickets will be resolved based on Government concurrence of project completion.
- All trouble tickets regardless of priority or project or percentage complete will be utilized and updated in the CSSP ticketing system until ticket closure. The contractor shall report tickets over 60 days on a weekly basis until completion/resolution.

3.5.5 On-Call Support

The contractor shall provide on-call support during non-core hours.

Support shall consist of fielding calls, initiating trouble tickets, and monitoring the progress of resolution on Critical and High priority issues that occur during non-core hours or occur during core hours and continue, unresolved, into non-core hours.

3.5.6 CSSP Subscriber Response

The contractor shall:

- Provide subscriber support and issue tracking for all subscribers
- Respond to subscribers' support requests within one (1) hour during core hours and open a trouble ticket within 90 minutes after 1st contact. Critical issues, including but not limited to a total loss of access to a subscriber facing application, or a compromise of any kind shall be acknowledged and remediation actions communicated (not necessarily remediation complete) as described in Table 4: Infrastructure Response Times. Medium/Low issues shall be deferred to core hours only and remediation times communicated to the Government for concurrence
- Document and share monthly percentages on the number of total subscriber calls received, tickets created, and issues resolved

3.5.7 Lead Systems Engineer

The Lead Systems Engineer shall:

- Review and track subscriber support issues and tickets and ensure timely follow-up and resolutions
- Engage other CSSP team members for troubleshooting applications that impact team resolution
- Ensure all configuration changes and system updates are properly vetted and aligned with configuration management requirements established by government
- Serve as a subject matter expert in system administration and network configuration
- Track project and project tickets and manage priorities ensuring deadlines are met
- Ensure attendance and participation in all meetings and briefings
  Ensure one Systems Engineer is on call 24/7/365

3.6 Boundary Assessment and Analysis Services

The Boundary Assessment Team (BAT) concentrates its efforts to the attack surface (public-facing assets) of the DREN. The BAT enumerates, identifies vulnerabilities, and validates cybersecurity compliance status in order to drive remediation activities, and reduce the overall cyber risk to the DREN. The area of operation consists of all publicly reachable services hosted on DREN. Information systems on DREN include but are not limited to Windows clients and servers, UNIX, Linux, Network Devices, Web Servers, Supercomputers, and a variety of software products. The Government estimates the DREN attack surface can vary +/- 10% at any given point in time.

BAT has a Government-provided Cloud Service Provider (CSP) platform in the public Internet and executes operations in the same manner as an adversary. Reconnaissance scans to discover the attack surface, technology enumeration, vulnerability assessments (agentless and absent of credentials), and security configuration validations are conducted to secure the attack surface.

In support of BAT activities, the contractor shall:

- Execute technical actions (scanning, software tool execution, script execution, etc.) to identify networks, hosts, technologies, software/hardware versions, vulnerabilities, etc.
- Conduct Open Source Intelligence (OSINT) on the target technology, network, application, etc.
- Develop a complete picture of the DREN public-facing attack surface using the information gained from these actions. The contractor shall ensure the discovery of the DREN attack surface is updated quarterly to ensure accuracy of results.
- Perform web application penetration testing against public-facing web applications on the DREN. The Government estimates that a third of web-enabled public-facing assets will require annual penetration testing.
- Perform security configuration validations in support of operations orders, directives, guidance, or taskings to include validation of remediation of Vulnerability Disclosure Program (VDP) findings within the applicable timeline as specified by JFHQ-DODIN. These assessments are typically a confirmation of a web setting or enumeration of a contractor product, for example.
- Perform cyber operations using documented TTPs to ensure high-quality and repeatable processes. If no applicable TTPs are available, the contractor shall document actual testing procedures and results and add those as new TTPs to the Government's repository prior to completion of the engagement.
- Provide direct subscriber support and issue tracking. The contractor shall track subscriber interaction through Government provided ticketing/issue tracking systems and provide sufficient documentation to allow for a third party to interpret the actions and status of the issue. The contractor shall include supporting artifacts or be referenced such that those artifacts can be retrieved and reviewed.
- Attend daily team synchronization calls, weekly status meetings, and briefings, in support of BAT operations.
- Perform a remote threat assessment of 40 service delivery points a year and provide a written report of findings and recommended remediation to new DREN and SDREN RDT&E subscribers, high risk subscribers and track to closure to reduce the risk posture of vulnerable sites.
- Validate the DREN and SDREN Attack Surface utilizing industry known best practices for defending network terrain by utilizing the Whitelist, Web, Email, DNS, FTP, DoD key task areas such as VPNs and public facing websites.
- Inventory public-facing assets, systems, and technologies within 120 days of contract start date and maintained the inventory throughout the contract period
- Conduct 6 penetration test engagements. These engagements could consist of multiple systems across multiple enclaves. The potential also exists for those engagements to exist on DOD or other Federal Government networks yet to be identified outside of DREN. The penetration testing would be conducted remotely with no travel required.
- Assess Cybersecurity Capabilities Implementation through validating and testing functionality of HBSS, ACAS, RADIX, and IDS implementation (e.g. coverage, configuration, etc.) "Mapping of the Lanes" (e.g. interconnectivity / overlays) and reporting finding alignment to the systems applicable RMF Scorecard and POA&M for tracking and closure based on risk level. Assessments will coordinate and identify security flaws and issues identified with the DoD Bug Bounty program.
- Follow a formal testing methodology and documented procedures to test systems vulnerabilities and misconfigurations, in order to maximize their reliability in the face of a cyber-attack and provide a written report of exploits and recommended remediation with mappings to STIGs, SRGs or NIST SP 800-53a rev4 controls and CCIs where applicable. The contractor assessment and analysis standards shall include remediation support, to ensure the appropriate mitigation occurs and the overall system risk is minimized.
- Prepare technical assessment reports for cybersecurity personnel and system administrators, and conduct formal briefings for effective communication of system analysis results to leadership. The site information and applicable IP ranges and equipment assessed will be provided by the Program Lead and through analyzing USCYBERCOM, JFHQ-DODIN, and SCC Orders such as Operation GHASTLY BASTION,

DoD Cybersecurity Campaign Plan / Cyber Scorecard, Internet-facing assets in STIG-compliant DMZ, Ports, Protocols, and Services Management (PPSM) and the DREN Whitelist. Provide AODR with report to brief connecting sites AO of findings.

The contractor shall ensure that at least one employee is available to review classified information on SDREN within two (2) hours of Government notification. This means the employee must be on-site with the necessary clearances and access.

3.6.1 CSSP Subscriber Response
The contractor shall:

- Provide subscriber support and issue tracking for all subscribers
- Respond to subscribers' support requests within one (1) hour during core hours and open a trouble ticket within 90 minutes after 1st contact during core hours. Requests during non-core hours may be deferred until the next working day
- Document and share monthly percentages on the number of total subscriber calls received, tickets created, and issues resolved

3.6.2 On-Call Support
The contractor shall provide on-call support during non-core hours.

Support shall consist of normal duties during non-core hours in the event of a cybersecurity event, named operation, or other activity requiring urgent actions.

3.7 Sustainment Services

The HPCMP CSSP subscriber base presently includes 158 subscribers of cybersecurity services. Sustainment services include, but are not limited to the following:

- Communicating with subscribers for coordination of Memorandums of Agreement (MOAs);
- Maintaining/coordinating current Point-of-Contact (POC) data for subscribers;
- Maintaining/coordinating current network diagrams for subscriber sites;
- Communicating with subscribers for the coordination of cybersecurity services;
- Maintaining listings and status of CSSP subscribers for communicating with Tier 1;
- Providing ongoing business communications with subscribers, including CSSP service pricing and invoice management and working with finance for funding coordination;
- Conducting sustainment requirements identified in the CSSP Evaluator's Scoring Metrics (ESM).

In support of these activities, the contractor shall:

- Maintain all current (up-to-date, reviewed yearly, etc.) written documentation (SOPs, Guidelines, Policies, Memos, Correspondence, etc.) for the CSSP Tier 1 and Tier 2, as required by the ESM. This document shall ensure the roles and responsibilities are clearly defined for organizations and sub-organizations within the Tier 1 and Tier 2 CSSPs and should be reviewed annually or at the request of the Government;
- Support re-certification or compliance validation through the documentation of processes and required deliverables;
- Establish, oversee, and deliver cybersecurity services to all new subscribers of services within thirty (30) days of established network connectivity to the DREN/SDREN, and ensure that existing subscribers do not have a lapse in service. This also includes service delivery performance monitoring and improvement. The contractor shall report weekly on the status of service establishment;
- Provide and follow a documented process for establishing services for subscribers. This process shall include subscriber agreements that are developed, coordinated, and signed by both the subscriber and the Government. The contractor shall ensure cybersecurity services initiated are in accordance with said agreement. Services provided are specifically assigned and documented in support of the subscriber responsibility to direct the security, operations, and defense of their portion of the DODIN. The contractor

shall review and validate the agreement at least annually. The contractor shall state other requirements in their developed documentation to include: six (6) month updates on points of contact and configuration changes, rollup of HBSS and vulnerability management feeds, and incident response services.

- The contractor shall collect subscriber's network diagrams and POC lists, and report monthly on the percentage that are current within six (6) months;
- Maintain current subscriber Memorandum of Agreements (MOAs), or appropriate substitution, signed by the HPCMP AO or formal designee. This document shall ensure the roles and responsibilities are clearly defined for organizations and sub-organizations.
- Provide and follow a documented process for establishing services for Subscribers. This process shall include subscriber agreements that are developed, coordinated, and signed by both parties.
- Ensure that the cybersecurity services initiated are in accordance with said agreement. Services provided are specifically assigned and documented in support of the Subscriber responsibility to direct the security, operations, and defense of their portion of the DODIN. The agreement shall be reviewed and validated annually, at a minimum.
- State other requirements in their developed documentation to include: 6 month updates on Points of Contact and configuration changes, rollup of HBSS and Vulnerability Management feeds, and incident response services.
- Ensure the following information is captured for each subscriber: scope and applicability of services are defined, general service (GENSER) designations, Supported Communications Circuit Service Designators (CCSDs), Authorizing Officials, Mission Criticality (as defined by the system owner), IP address ranges, Physical locations, Subscriber Points of Contact, Identification of any backend connections.
- Ensure that Subscriber/Provider roles and responsibilities are clearly defined.
- Validate annually that the organization is delivering all services identified in policy documentation and agreements with Subscribers
- Ensure the following information is captured for each subscriber: scope and applicability of services are defined, GENSER/SE designations, DREN Portal IDs, Authorizing Officials, Mission Criticality (as defined by the system owner), IP address ranges, Physical locations, subscriber Points of Contact, Identification of any backend connections. The contractor shall ensure that subscriber/provider roles and responsibilities are clearly defined. The contractor shall validate annually that all services identified in policy documentation and agreements with subscribers are being delivered.
- Prepare documentation and coordinate activities associated with DoD evaluation and inspection activities.

3.7.1 CSSP Subscriber Response

The contractor shall:

- Provide subscriber support and issue tracking for all subscribers
- Respond to subscribers' support requests within one (1) hour during core hours and open a trouble ticket within 90 minutes after 1st contact during core hours. Requests during non-core hours may be deferred until the next working day
- Document and share monthly percentages on the number of total subscriber calls received, tickets created, and issues resolved

4 Special Requirements

This section describes the special requirements for this effort. The following sub-sections provide details of various considerations on this effort.

4.1 Security and Safety

This section describes the security and safety for this effort. The following sub-sections provide details of various considerations on this effort.

4.1.1 Safety

Contractor Compliance: The contractor and its subcontractors shall comply with Public Law 91-596 (Occupational Safety and Health Act (OSHA)) and the Environmental, Safety, and Occupational Health (ESOH) (DODD 4715.1E). These requirements shall be incorporated into the contractors' safety and health program. The Department of Defense (DOD) participates in the OSHA Voluntary Protection Program (VPP). Contractor personnel

performing services on a DoD installation shall participate in the local VPP. Information on the VPP is available at http://www.osha.gov/dcsp/vpp/index.html.

Mishap Notification and Investigation: The contractor and its subcontractors (if applicable) shall promptly report pertinent facts regarding mishaps involving Government property damage or injury to Government personnel and to cooperate in any resulting safety investigation. The contractor shall notify (via telephone) the cognizant PCO, COR, and/or other applicable members within four (4) hours of all mishaps or incidents. The Government person notified by the contractor will in-turn notify the Safety office. Contractor notifications made after duty hours shall be reported to the appropriate installation Command Post. If requested by the cognizant PCO, the COR, and/or the cognizant program manager, the contractor shall immediately secure the mishap scene/damaged property and impound pertinent maintenance and training records until released by the investigating safety office. If the Government investigates the mishap, the contractor and the subcontractors shall cooperate fully and assist the Government personnel until the investigation is completed.

4.1.2 Onsite Access

The Government has the right to restrict on-site access to any contractor personnel who is identified as a potential threat to the health, safety, security, or operational mission of the Corps of Engineers.

4.1.3 Access to Certain Restricted Areas

Certain facilities, buildings or rooms are restricted to only individuals with proper security clearance. When the Contractor employees are required to perform work in these sensitive areas, they shall be escorted at all time by an authorized Government employee. Other sensitive areas may require only pre-clearance of one or more particular Contractor employees.

4.1.4 Access to Government Information Systems

All contractor employees with access to a Government information system must successfully complete the DoD Information Assurance Awareness training prior to access to the information system and then annually thereafter.

4.1.5 AT Level I Training

All contractor employees, to include subcontractor employees, requiring access to Army installations, facilities, controlled access areas, or require network access, shall complete AT Level I awareness training within 30 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. Upon request, the contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the COR or to the PCO (if a COR is not assigned), within 5 calendar days after completion of training by all employees and subcontractor personnel. AT Level I awareness training is available at the following website: https://jko.jten.mil/courses/AT-level1/launch.html; or it can be provided in presentation form which will be documented via memorandum.

4.1.6 Access and General Protection/Security Policy and Procedures

All contractor and all associated sub-contractors employees shall comply with applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by Government representative). The contractor shall also provide all information required for background checks or background investigation and to meet installation/facility access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any installation or facility change, the Government may require changes in contractor security matters or processes.

4.1.7 iWATCH Training

The contractor and all associated sub-contractors shall brief all employees on the local iWATCH, Corps Watch, or See Something, Say Something program (training standards provided by the requiring activity ATO). This local developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within 30 calendar days of contract award

and within 30 calendar days of new employees commencing performance with the results reported to the COR NLT 5 calendar days after contract award.

4.1.8 Contractor Employees Who Require Access to Government Information Systems
All contractor employees with access to a Government information system must be registered in the Army Training Certification Tracking System (ATCTS) at commencement of services, and must successfully complete the DOD Information Assurance Awareness prior to access to the information systems and then annually thereafter in accordance with personnel security standards listed in AR 25-2 (Information Assurance), an appropriate background investigation will be conducted prior to accessing the Government information systems.

4.1.9 Contracts that Require an OPSEC Standing Operating Procedure/Plan
The Contractor shall develop an OPSEC SOP/Plan within 90 days of contract award. The OPSEC SOP/Plan must be reviewed and approved by the RA OPSEC Officer. The SOP/Plan will include 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. In addition, the contractor shall identify an individual who will be an OPSEC Coordinator.

4.1.10 Contracts that Require OPSEC Training
All new contractor employees will complete Level I OPSEC Training within 30 calendar days of their reporting for duty. Additionally, all contractor employees must complete annual OPSEC awareness training. The contractor shall submit certificates of completion for each affected contractor and subcontractor employee, to the COR or to the PCO (if a COR is not assigned), within 5 calendar days after completion of training. OPSEC awareness training is available at the following websites: https://www.iad.gov/ioss/ or http://www.cdse.edu/catalog/operations-security.html; or it can be provided by the RA OPSEC Officer in presentation form which will be documented via memorandum.

4.1.11 Information Assurance (IA)/Information Technology (IT) Certification
All contractor employees and associated subcontractor employees shall complete the DoD Information Assurance (IA) awareness training before issuance of network access and annually thereafter. Per DoD 8570.01-M, DFARS 252.239-7001 and AR 25-2, all contractor employees supporting IA/IT (Information Technology) functions shall be appropriately certified upon order award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon order award. Table 5: DoD 8570.01-M Requirements is provided for reference as the minimum acceptable certification level.

Table 5: DoD 8570.01-M Requirements

Major Requirement	Required DoD 8570.01-M Certification
Boundary Assessment Services	IAT-II and CSSP Auditor
Warning Intelligence Services	IAT-II and CSSP Analyst or CSSP Incident Responder
Protect Services	IAT-II and CSSP Analyst or CSSP Incident Responder
Detect Services	IAT-II and CSSP Analyst or CSSP Incident Responder
Sustainment Services	IAM-I
Infrastructure Services	IAT-II and CSSP Infrastructure Support

4.1.12 Access to Classified Information
Contractor shall comply with AR 380-67 (Personnel Security Program) and Homeland Security Presidential Directive 12 (Policy for a Common Identification Standard for Federal Employees and Contractors) as well as FAR 52.204-2, Security Requirements. Additionally, Contractors shall comply with The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); any revisions to DOD 5220.22-M, notice of which has been furnished to the contractor. The DD Form 254 will be attached with the contract.

4.1.13 Classified and/or Sensitive Materials and/or Sensitive or Restricted Areas
All contract employees, including subcontractor employees who are not in possession of the appropriate security clearance, will be escorted in areas where they may be exposed to classified and/or sensitive materials and/or sensitive or restricted areas.

4.1.14 Pre-screen candidates using E-Verify Program

The Contractor must pre-screen Candidates using the E-verify Program (http://www.uscis.gov/e-verify) website to meet the established employment eligibility requirements. The Vendor must ensure that the Candidate has two valid forms of Government issued identification prior to enrollment to ensure the correct information is entered into the E-verify system. An initial list of verified/eligible Candidates must be provided to the COR no later than 3 business days after the initial contract award.

4.1.15 Threat Awareness Reporting Program

All new contractor employees will complete annual Threat Awareness and Reporting Program (TARP) Training provided by a Counterintelligence Agent, IAW AR 381-12 . The contractor shall submit certificates of completion for each affected contractor and subcontractor employee(s) or a memorandum for the record, to the COR or to the contracting officer (if a COR is not assigned), within 5 calendar days after completion of training. Authorized webbased TARP training and Quiz is available at the following website:
https://www.youtube.com/watch?v=K0uXaT6Ps1w
Quiz: https://securityawareness.usalearning.gov/itawareness/index.htm

4.1.16 Clearances

The Prime Contractor Company and subcontractors working in areas that require access to classified information must have a Facility Clearance (FCL) at the appropriate level (IAW the NISPOM DOD 5220.22-M and AR 380-49) in order to perform the requirements of this contract. Contractor personnel performing work under this contract must have the required security clearance, per AR 380-67, at the appropriate level at the start of the period of performance. Security Clearances and FCL requirements are required to be maintained for the life of the contract IAW the DD254 attached to the contract. DD Forms 254: Overarching security requirements and Contractor access to classified information shall be as specified in the basic DD Form 254. **(AM #0002)** Joint Venture (JV) offeros shall comply with the 2020 NDAA and 13 C.F.R. Section 121.103(h)(4) in meeting these requirements. **(AM #0002)**

Contractor and employees of the contractor are required to be citizens of the United States and must maintain such status during the duration of this contract. In accordance with DoD 5200-2.R, all persons (DoD military, civilian, and contractor personnel) using unclassified automated information systems must have at a minimum a positive National Agency Check with Local Agency and Credit Checks (NACLC). The contractor shall submit verification that this checks has been submitted for each contractor employee on the task prior to beginning work on the task. Contractor employees are required to possess a “secret” or “top secret” security clearance as specified in Security Clearances (0).

4.1.16.1Visitor Group Security Agreement

The contractor shall sign a Contractor Visitor Group Security Agreement to protect classified information involved in performance under this contract. The Agreement will outline responsibilities in the following areas: Contractor security supervision; Standard Practice Procedures; access, accountability, storage, and transmission of classified material; marking requirements; security education; personnel security clearances; reports; security checks; security guidance; emergency protection; protection of Government resources; DD Forms 254; periodic security reviews; and other responsibilities, as required.

4.2 Government Furnished Property

4.2.1 Government Furnished Property

The Government will make available the following property to the contractor for use on contract:

- Computers and similar equipment.
- Office space, utilities, and office supplies for use at Government locations
- Office furniture and other office equipment (i.e. calculators, typewriters, telephones, safes/storage equipment for use at Government locations

4.2.2 Property Accountability

The contractor shall be responsible for all Government-furnished property assigned to employees of this contract. The contractor shall provide appropriate documentation for property within his/her possession. The contractor shall

be required to sign documentation when Government property is in transit or temporarily in contractor possession. The contractor shall conduct an inventory of all Government-furnished equipment annually and provide inventory results to the designated Property Hand Receipt Holder.

4.3 Contractor Furnished Property

The contractor shall furnish any specialized equipment deemed by the contractor to be necessary for contract compliance, for the use of employees employed under this contract. The Government will not separately reimburse the Contractor for any contractor furnished property.

4.4 Scope Changes

Any matter concerning a change to the scope, prices, terms, or conditions of this contract shall be referred to the PCO and not the COR.

4.5 Performance Evaluation

The contractor's performance of services will be evaluated as defined in the Quality Assurance Surveillance Plan (QASP).

4.6 Phase-in/Phase-out

The Contractor shall perform the activities necessary to effectively and efficiently Phase-in/Phase-out resources and personnel onto this contract and ensure full continuity of CSSP support to the Government. Prior to the termination of this contract, the Contractor shall perform the contract phase-out activities necessary to support the transition of services to a follow-on provider.

4.7 Employee Conduct

When contractor employees are working on Government facilities or participating at Government meetings, they shall wear identification badges distinguishing themselves as such and expected to conduct themselves IAW DoD workplace rules and regulations. The badges at a minimum must have the employee's name and word "contractor" displayed. Ideally, the company name will appear on the badge. Additionally, notwithstanding any other provisions in the PWS, the contractor shall identify himself as a contractor in meetings, telephone conversations, all written communications, and work situations so their actions cannot be construed as acts of a Government official. The contractor shall take no actions that bind the Government to a final decision or results in the exercise of Government discretion.

4.8 Security Incidents

The contractor shall report any compromise or possible compromise of classified or CUI item, material, or information to the cognizant security office(s) listed on the contract DD Form 254 as well as the HPCMP upon discovery of the incident.

4.9 Applicable Directives

The contractor shall comply with all regulations, directives, and documents referenced in this PWS. If these documents are revised or superseded, the contractor shall comply with the revised document or the document which superseded it.

4.10 Order-Level Materials (OLM)

The contractor may be required to obtain contract related materials, i.e., supplies, equipment, software, licenses, etc., to support the overall requirement. The Contractor shall abide by the requirements of the FAR and other DOD Mandatory sources/contractual vehicles when acquiring supplies and/or materials. The Contractor shall obtain three (3) quotes in accordance with the FAR from suppliers. The contractor shall include documentation of these quotes and submit for approval by the PCO. Documentation of purchases will be input into the agency's reporting system in order for the Government to review them upon request and to ensure compliance with Federal procurement regulations. All supplies must be authorized by the COR or PCO and be in compliance with this contract and all other applicable requirements.

Additionally, the contractor will be required to give first consideration to Army Computer Hardware, Enterprise Software and Solutions (CHESS) contracts/blanket purchase agreements when purchasing hardware and software. The following statements/clauses from CHESS contracts will apply:

4.11 IT Equipment/Software Solutions

All materials required for performance of the contract, which are not Government-furnished, shall be furnished by the contractor. Materials acquired by the contractor with Government funds, for performance of this contract, are the property of the Government. The contractor shall utilize Enterprise Software Initiative (ESI) source software and Computer Hardware, Enterprise Software and Solutions (CHESS) contract source equipment in accordance with applicable provisions in Section H, CHESS Source Contracts and DoD ESI. In addition to any other equipment, the contractor shall separately identify ESI source software items and CHESS contract source equipment in each TO proposal. For ESI source software, the contractor shall request approval to order from the Government supply sources. For proposed materials that are not from the identified Government supply sources for ESI source software or CHESS contract source equipment, the contractor shall provide a justification why those sources are not being utilized to support approval by the PCO. Contractor costs for ESI source software shall be reimbursed at the prices charged to the contractor, with no mark-up percentage for loadings, fee or profit, regardless of whether the contract type of the contract is Fixed Price or Cost Reimbursable. For CHESS contract source equipment, a fixed mark-up percentage for associated indirect loading shall be applied to the CHESS contract source equipment for FP contracts; however, profit or fee shall not be allowed. Advanced planning and earlier initiation of purchase request process for known procurements will be incentivized. This will be reflected by eliciting multiple contractor quotes from CHESS and industry ensuring the best value to the Government. It must be apparent that the contractor has afforded the process enough time for quotes to come in with 0% delay to schedule, by starting the process well in advance of imminent need. Cost Savings in this case must be quantified and presented to the Government in the quarterly reviews.

5 Deliverables

The contractor shall research, develop, prepare or write, and submit the deliverables identified in this section. Contractor format is acceptable unless another format is specified by the COR. All deliverables shall be delivered to the COR in the manner specified by the COR (email, shared drive, or other as applicable). If the Government determines the deliverable needs to be corrected, upon COR notification, the contractor shall be required to re-submit the corrected deliverable within five (5) business days.

4.8 Major Requirements Deliverables

The contractor shall prepare the following deliverables per the identified frequency. Content, format, storage location, and specific delivery date/time shall be identified by the COR or other designated Government representative.

Table 6: Program Manager Deliverables

PROGRAM MANAGER (PWS 3.1)		
Identifier	**Description**	**Frequency**
A001	Metrics in support of Quarterly Quality Assurance (QA) Program	Quarterly
A002	Metrics in support of Ad-Hoc Authorizing Official (AO) Report	Ad-hoc
A003	Monthly Staffing Report	Monthly
A004	Report of Issues	Ad-hoc
A005	Program Documentation	Ad-hoc
A006	Staff Listing and Organization Chart	Ad-hoc

Table 7: Detect Services Deliverables

DETECT SERVICES (PWS 3.2)		
Identifier	**Description**	**Frequency**
B001	Incident and Event Reports	Ad-hoc
B002	After Action Reports (AARs) and Lessons Learned	Ad-hoc
B003	Collaboration and Information Sharing	Ad-hoc
B004	Standard Operating Procedure (SOP) and Tactics, Techniques, and Procedure (TTP) Documentation	Ad-hoc

B005	Effectiveness of Security Controls Report	Monthly
B006	Quality Assurance Report	Weekly
B007	Countermeasure Deployment Report	Monthly
B008	Program Documentation – Project documentation, including formal briefings and information papers, training documents, incident and event analysis reporting, exercise planning	Ad-hoc

Table 8: Warning Intelligence Services Deliverables

WARNING INTELLIGENCE SERVICES (PWS 3.3)		
Identifier	**Description**	**Frequency**
C001	Analysis Reports	Ad-hoc
C002	After Action Reports (AARs) and Lessons Learned	Ad-hoc
C003	Collaboration and Information Sharing	Ad-hoc
C004	Standard Operating Procedure (SOP) and Tactics, Techniques, and Procedure (TTP) Documentation	Ad-hoc
C005	Intrusion Detection Sensor Dashboards and Alerts Developed	Ad-hoc
C006	Subscriber Technical Risk Reports	Ad-hoc
C007	Forensic Reports	Ad-hoc
C008	APT Research and Briefings	Ad-hoc

Table 9: Protect Services Deliverables

PROTECT SERVICES (PWS 3.4)		
Identifier	**Description**	**Frequency**
D001	Analysis Reports (Vulnerability Analysis, ISCM reports, Insider Threat, etc.)	Ad-hoc
D002	AARs and Lessons Learned	Ad-hoc
D003	Collaboration and Information Sharing	Ad-hoc
D004	Standard Operating Procedure (SOP) and Tactics, Techniques, and Procedure (TTP) Documentation	Ad-hoc
D005	Program Documentation – Project documentation, including formal briefings and information papers, as well as metrics provided for Quality Assurance reviews	Ad-hoc
D006	Vulnerability and Discovery Scan Reports – Vulnerability Scan reports delivered to subscribers in accordance with USCYBERCOM guidance	Monthly
D007	ISCM Reports – delivered to subscribers	Monthly
D008	ESS Agent and Module Deployment Report – Report showing compliance with orders relating to endpoint security systems	Monthly
D009	Acknowledgement Report (IAVM, ISCM, CPCON) – Report showing subscriber acknowledgement of orders/reports	Monthly
D010	Credentialed Scan Failure Reports – delivered to subscribers	Monthly
D011	ACEM Compliance Report – delivered to subscribers	Monthly
D012	Site Initiation Report	Weekly

Table 10: Infrastructure Services Deliverables

INFRASTRUCTURE SERVICES (PWS 3.5)		
Identifier	**Description**	**Frequency**
E001	Change management request report	Ad-hoc
E002	COOP documentation and test reports	Ad-hoc
E003	Incomplete/Unresolved tickets over 60 days	Weekly
E004	After Action Reports (AARs) and Lessons Learned	Ad-hoc
E005	Collaboration and Information Sharing	Ad-hoc

E006	Standard Operating Procedure (SOP) and Tactics, Techniques, and Procedure (TTP) Documentation	Ad-hoc
E007	Compliance Metrics Report	Ad-hoc

Table 11: Boundary Assessment and Analysis Services Deliverables

BOUNDARY ASSESSMENT AND ANALYSIS SERVICES (PWS 3.6)		
Identifier	**Description**	**Frequency**
F001	Standard Operating Procedure (SOP) and Tactics, Techniques, and Procedure (TTP) Documentation	Ad-hoc
F002	Penetration Testing Report	Ad-hoc
F003	Attack Surface Data (raw and modified data)	Ad-hoc
F004	Results of testing documented in HPCMP's ticketing system	Ad-hoc
F005	BAT Boundary Report	Monthly
F006	After Action Reports (AARs) and Lessons Learned	Ad-hoc
F007	Collaboration and Information Sharing	Ad-hoc

Table 12: Sustainment Services Deliverables

SUSTAINMENT SERVICES (PWS 3.7)		
Identifier	**Description**	**Frequency**
G001	Analysis Reports	Ad-hoc
G002	AARs and Lessons Learned	Ad-hoc
G003	Program Documentation such as templates, SOPS and TTPS in support of mission directed by Program Lead	Ad-hoc
G004	Training Plan	Ad-hoc
G005	Workforce Plan	Ad-hoc
G006	Site Initiation and Service Establishment Report	Weekly
G007	Report of percentage of network diagrams and POC lists that are current within six (6) months	Weekly
G008	Monthly ATCTS reporting	Monthly
G009	Repository update of subscriber network diagrams	Semi-annually
G010	Repository update of Subscriber POC listing	Semi-annually
G011	CSSP Handbook (including pricing sheet) update	Annually
G012	Validation that services identified in policy documentation and agreements with subscribers are being delivered	Annually

4.8 CSSP Operational Update

The contractor shall prepare a CSSP Operational Update that captures relevant weekly metrics and significant highlights, accomplishments, and issues from each major requirement, and deliver it at least one (1) hour prior to the weekly scheduled operational status update meeting. Report content, format, and storage location shall be identified by the COR or designated Government representative.

5.3 Work Availability Schedule

The contractor shall prepare and deliver a work availability schedule for the upcoming service month two (2) business days prior to the start of the next service month to the COR.

5.4 Monthly Status Report

The contractor shall deliver a Monthly Status Report (MSR) no later than the 10th calendar day of the following month. At a minimum, the MSR shall include:

- Relevant metrics (number of incidents, trouble ticket status, alert statistics, etc.) for each major requirement;
- Quality assurance metrics by analyst;
- Status of outstanding deliverables;
- Status of projects, if any, with assigned employees;

- Actual versus planned travel and surge labor hour expenditures;
- Staff listing by major requirement with any applicable staffing status (new hires, vacancies, etc.). If this listing shows that less than 95% of the positions are filled within thirty (30) days, the contractor shall explain why and identify when they will be fully staffed;
- 8570 Certification status by employee. If this status shows that less than 100% of the staff is certified in accordance with DoD 8570, the contractor shall explain why and identify when their staff will be 100% certified.
- Current staffing levels to include vacancies, excepted onboarding dates of new employees, and any employees schedule to depart.

5.5 Government Furnished Property Inventory

The contractor shall maintain an inventory of Government Furnished Property (GFP) that has been issued to them, and deliver a report no later than the 10th calendar day of the month following the end of every six (6) months beginning on the start of the order to the COR.

5.6 Report/Record of Meeting Minutes

When requested by the Government, the contractor shall attend regularly scheduled or impromptu program, management, or contract meetings. If meeting minutes are required, the deliverable shall document key findings/action items and information on program schedules, milestones, potential risks and troubleshooting measures, problem resolution, current status of tasking, and other supporting information. The contract deliverables for meeting minutes are identified in the below subsections. Should the COR require other meeting minutes as a deliverable, the COR will notify the contractor in advance of the meeting.

a. Contract Kick Off Meeting

Immediately upon award notification, the contractor shall meet with the Government to discuss the transition needs. Within fifteen (15) business days following the order award date, the contractor shall meet with the COR and the PCO to review all goals and objectives, terms and conditions of this order, and discuss technical requirements. The contractor shall deliver the meeting minutes no later than five (5) business days after meeting completion.

b. Semi-Annual Performance Review

The contractor shall meet with the Government via teleconference or on-site at a location determined by the Government to discuss the contractor's current performance under this order. The Government will schedule the semi-annual performance review at least ten (10) business days in advance of the meeting, and the contractor shall provide read-ahead material to the Government and the PCO for review at least five (5) business days in advance of the scheduled meeting. The review shall report the current status of performance requirements, goals, and objectives. The contractor shall report any issues, risks, or conditions impacting current performance and a planned course of action for their resolution. The contractor shall deliver the meeting minutes no later than five (5) business days after meeting completion.

5.7 Quality Control Plan

The contractor shall prepare and deliver a QCP to the PCO for review and acceptance within ten (10) business days after contract award. The PCO will notify the contractor of acceptance or required plan changes. If changes are required, the contractor shall make them within ten (10) business days and resubmit for PCO review and acceptance. 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 he assures himself that his work complies with the requirement of the contract. The contractor shall maintain this plan throughout the life of this order with delivery to the PCO within thirty (30) calendar days after an update. Contractor format is acceptable, but the plan must, at a minimum, address the items listed below.

- A description of the inspection system to cover all major services and deliverables. The description shall include specifics as to the areas to be inspected on both a scheduled and unscheduled basis, frequency of inspections, and the title of inspectors.
- A description of the methods to be used for identifying and preventing defects in the quality of service performed.

- A description of the records to be kept to document inspections and corrective or preventative actions taken.
- All records of inspections performed shall be retained and made available to the Government upon request throughout the task order performance period, and for the period after task order completion, until final settlement of any claims under this task order.

5.8 Contractor Performance

Table 13: Performance Requirements Matrix identifies the acceptable quality level for each major requirement that is considered critical to the success of the contract. All subordinate paragraphs under the PWS reference column apply.

5.9 Quality Assurance

The Government will evaluate the contractor's performance of this order using the performance objectives of this order, the Government's Quality Assurance Surveillance Plan (QASP), and the contractor's approved QCP. The Government reserves the right to inspect any service or deliverable in accordance with the inspection clauses applicable in the basic contract and this order. Government surveillance of tasks not listed in the Performance Matrix or by methods other than those listed in the Performance Matrix (such as provided in the inspection clauses) may occur during the performance period of this order. For those tasks listed in the Performance Matrix, the COR or other designated evaluator will follow the method of surveillance specified in this order (e.g., Subscriber Complaint/Survey process, Periodic surveillance, Random monitoring, or 100 percent inspection). Government personnel will record all surveillance observations. When an observation indicates defective performance, the COR or other designated evaluator will require the contractor manager or representative at the site to initial the observation. The initialing of the observation does not necessarily constitute concurrence with the observation. It acknowledges that the contractor has been made aware of the non-compliance. Upon receipt of such notification, the Contractor shall correct the deficiency within the time specified by the COR. However, in the event that the deficiency represents a hazard to health or safety, or it serves to jeopardize operational continuity, then corrective action shall proceed immediately and continue uninterrupted until the correction is affected. In all cases, the correction of performance deficiencies shall not in any way adversely affect other contract performance. In some instances and in coordination with the Small Business Administration, contractor payment may be delayed or reduced until the deficiency is cured. Any action taken by the PCO as a result of surveillance will be according to the terms of the order and/or basic contract.

Table 13: Performance Requirements Matrix

PWS Reference	Deliverable or Service	Performance Standard	Acceptable Quality Level (AQL)	Method of Surveillance
3.2	Detect Services	Contractor analysts complete a Joint Qualification Requirements (JQR) process to ensure their analysis of Intrusion Detection System (IDS) alerts to identify unauthorized or anomalous activity are categorized correctly.	Every analyst must pass the JQR within 90 days of assignment.	100% Inspection
3.2	Detect Services	The contractor reviews alerts to identify unauthorized or anomalous activity, and takes action.	Critical and High alerts are reviewed within fifteen (15) minutes of entering the security information and event management (SIEM) tool. Medium alerts shall be reviewed within forty-five (45) minutes of entering the SIEM. Low alerts shall be reviewed within one (1) hour of entering the SIEM.	Periodic Inspection
3.2	Detect Services	The contractor responds to alerts to characterize and categorize the alert for action.	Critical and High priority alerts reviewed and adjudicated within thirty (30) minutes of entering the SIEM. Medium alerts reviewed and adjudicated within ninety (90) minutes and low alerts reviewed and adjudicated within twelve (12) hours of entering the SIEM.	Periodic Inspection
3.2	Detect Services	The contractor creates incident response tickets within timelines outlined in CJCSM 6510.01B.	97% of incidents and events are processed within the minimum reporting timelines in CJCSM 6510.01B.	100% Inspection
3.2	Detect Services	Ensure that reports are peer-reviewed and less than 10% of reports are rejected due to error.	Less than 10% of the reports processed are rejected due to error.	100% Inspection
3.2.3	Detect Services, CSSP Subscriber Response	The contractor responds to subscriber support requests within one (1) hour during core hours and opens a ticket within ninety (90) minutes after 1st contact	95% response rate to subscriber requests within defined timelines	Periodic Inspection
3.3	Warning Intelligence Services	The contractor reviews all intelligence tippers and bulletins, and drafts the accompanying signatures within twenty-four (24) hours from the time that intelligence is received.	90% of signatures are developed within the required timeline.	Periodic Inspection
3.3	Warning Intelligence Services	Contractor analysts complete a Joint Qualification Requirements (JQR) process	Every analyst must pass the JQR within 90 days of assignment.	100% Inspection
3.3.1	Warning Intelligence Services, CSSP Subscriber Response	The contractor responds to subscriber support requests within one (1) hour during core hours and opens a ticket within ninety (90) minutes after 1st contact	95% response rate to subscriber requests within defined timelines	Periodic Inspection
3.4	Protect Services	Contractor analysts complete a Joint Qualification Requirements (JQR) process	Every analyst must pass the JQR within 90 days of assignment.	100% Inspection
3.4.2	Protect Services, Vulnerability	The contractor configures all ACAS Monthly Vulnerability and Discovery	95% of scans are performed as credentialed scans.	Periodic Inspection

PWS Reference	Deliverable or Service	Performance Standard	Acceptable Quality Level (AQL)	Method of Surveillance
	Assessment and Analysis	Scans to meet USCYBERCOM guidance.		
3.4.3	Protect Services, Vulnerability Management	The contractor monitors and tracks subscriber compliance with IAVA alerts and compliance deadlines.	95% subscriber compliance with published INFOCON and IAVM notifications within the required timeline.	Periodic Inspection
3.4.4	Protect Services, Endpoint Protection	The contractor performs proper implementation and maintenance of DoD mandated and approved enterprise end point protection.	95% of subscribers' hosts compliant with relevant endpoint TASKORDS.	Periodic Inspection
3.4.6	Protect Services, Information Security Continuous Monitoring (ISCM)	The contractor monitors and tracks subscriber acknowledgment of ISCM reports	90% subscriber acknowledgment of ISCM reports.	Periodic Inspection
3.4.8	Protect Services, CSSP Subscriber Response	The contractor responds to subscriber support requests within one (1) hour during core hours and opens a ticket within ninety (90) minutes after 1st contact	95% response rate to subscriber requests within defined timelines	Periodic Inspection
3.5	Infrastructure Services	Upon discovery of a Critical issue, the contractor opens a ticket for action within thirty (30) minutes during core hours and within one (1) hour during non-core hours. Upon discovery of a High issue, the contractor opens a ticket for action within one (1) hour during core hours and within two (2) hours during non-core hours.	97% of the tickets are opened within the required timeline.	Periodic Inspection
3.5.1	Infrastructure Services, Operations	The contractor applies and maintains cybersecurity for CSSP systems, and ensures business continuity for cybersecurity operations and IT systems.	ACAS servers are setup and shipped within 72 hours of new subscriber notification from CSSP Sustainment.	Period Inspection
3.5.2	Infrastructure Services, Security	Unless directed by the Government, the contractor ensures all CSSP systems are no less than 90% IAVA compliant, 90% STIG compliant, and all Critical and CAT I findings are remediated within one (1) week of discovery.	90% of all CSSP systems are IAVA and STIG compliant with no open Critical or CAT I findings.	Periodic Inspection
3.5.2	Infrastructure Services, Security	Unless directed by the Government, the contractor ensures all CSSP systems are no less than 95% of systems are scanned with credentials	95% of all CSSP systems are scanned with valid credentials	Periodic Inspection
3.5.3	Infrastructure Services, Continuity of Operations (COOP)	In disaster recovery and exercise situations, the contractor executes COOP and restores: - Tier 1 capability within three (3) hours regardless of core or non-core hours. Tier 2 capability within two (2) days.	99% of capabilities are restored within the required timeline.	100% Inspection

PWS Reference	Deliverable or Service	Performance Standard	Acceptable Quality Level (AQL)	Method of Surveillance
3.5.4	Infrastructure Services, Issue Tracking	If equipment replacement is required, the contractor shall notify the equipment contractor and execute return material authorization (RMA) procedures within 24 hours of discovery.	90% of replacement equipment is requested within the required timeline.	Periodic Inspection
3.5.4	Infrastructure Services, Issue Tracking	The contractor installs replacement equipment within 24 hours of receipt of the equipment.	90% of replacement equipment is installed within the required timeline.	Periodic Inspection
3.6	Boundary Assessment Services	The contractor shall ensure the discovery of the DREN attack surface is updated quarterly to ensure accuracy of results.	95% of Quarterly reports are received and updated.	Periodic Inspection
3.6	Boundary Assessment Services	The contractor shall perform security configuration validations in support of operations orders, directives, guidance, or taskings to include validation of remediation of Vulnerability Disclosure Program (VDP) findings within the timeline defined by JFHQ-DoDIN.	95% of validations are performed within the timeline of the order.	Periodic Inspection
3.6	Boundary Assessment Services	The contractor shall perform a remote threat assessment of 40 service delivery points a year and provide a written report of findings and recommended remediation to new DREN and SDREN RDT&E subscribers, high risk subscribers and track to closure to reduce the risk posture of vulnerable sites	95% of threat assessments are conducted annually.	100% Inspection (annual review)
3.6	Boundary Assessment Services	The contractor shall conduct six (6) penetration test engagements	100% of engagements are conducted annually.	100% Inspection (annual review)
3.6	Boundary Assessment Services	The contractor shall inventory public-facing assets, systems, and technologies within 120 days of contract start date and maintained the inventory throughout the contract period	100% inventory.	100% Inspection (annual review)
3.6.1	Boundary Assessment Services, CSSP Subscriber Response	The contractor responds to subscriber support requests within one (1) hour during core hours and opens a ticket within ninety (90) minutes after 1st contact	95% response rate to subscriber requests within defined timelines	Periodic Inspection
3.7	Sustainment Services	The contractor maintains written documentation for the CSSP Tier 1 and Tier 2, as required by the ESM.	CSSP Handbook, Training Plan, and Workforce Plan are reviewed and updated annually or at the request of the Government	100% Inspection (annual review)
3.7	Sustainment Services	The contractor collects subscriber's network diagrams and POC lists, and report monthly on the percentage that are current within six (6) months.	95% of subscriber's network diagrams and POC listings in the repository are up-to-date and are as described by the subscriber	100% Inspection (semi-annual review)
3.7.1	Sustainment Services, CSSP Subscriber Response	The contractor responds to subscriber support requests within one (1) hour during core hours and opens a ticket	95% response rate to subscriber requests within defined timelines	Periodic Inspection

PWS Reference	Deliverable or Service	Performance Standard	Acceptable Quality Level (AQL)	Method of Surveillance
		within ninety (90) minutes after 1st contact		
5.1	Major Requirement Deliverables	Documentation is accurate, professionally prepared, and easily understood. Delivery within the required frequency/timelines.	On-time delivery at 90% level.	Periodic Inspection
5.2	CSSP Operational Update	Documentation is accurate, professionally prepared, and easily understood. Delivery at least one (1) hour prior to the weekly scheduled operational status update meeting.	On-time delivery at 90% level.	Periodic Inspection
5.3	Work Availability Schedule (monthly)	Documentation is accurate, professionally prepared, and easily understood. Delivery two (2) business days prior to the start of the next service month.	On-time delivery at 90% level.	100% Inspection
5.4	Monthly Status Report (MSR)	Documentation is accurate, professionally prepared, and easily understood. Delivery no later than the 10th calendar day of the following month.	On-time delivery at 90% level.	100% Inspection
5.5	Government Furnished Property Inventory	Documentation is accurate, professionally prepared, and easily understood. Delivery no later than the 10th calendar day of the month following the end of every six (6) months beginning on the start of the order	On-time delivery at 90% level.	100% Inspection

SECTION L - INSTRUCTIONS, CONDITIONS AND NOTICES TO BIDDERS

The following have been modified:

SECTION L

A. PROPOSAL SUBMISSION (FAR 52.212-1)

1. PROPOSAL SUBMISSION REQUIREMENTS

a. Overview. Interested firms or joint venture entities (here after referred to as Offerors) must submit proposals demonstrating their capability to successfully execute the contract resulting from this solicitation. The Government will evaluate the proposals in accordance with the criteria described herein. This is a "Best Value" solicitation for W912HZ22R0007 HPCMP CSSP Support Services. The Government will evaluate proposals in accordance with the criteria described herein, and award a firm fixed price contract to the responsible offeror whose proposal conforms with all the terms and conditions of the solicitation and whose proposal is determined to represent the overall best value to the Government utilizing the trade-off process described in FAR 15.101-1.

b. Description of Work. This procurement will allow the HPCMP to continue to provide engineering, design and development of tools and processes through the examination and establishment of new methods for cybersecurity deterrence, protection, detection, and adaptation using advanced cybersecurity assessment techniques, as well as to provide services for the evaluation of large-scale cyber data sets using advanced and predictive analytics.

c. Copies of Solicitation Documents and Amendments. Copies of the solicitation and amendments are available by INTERNET ACCESS ONLY. All solicitation documents will be posted to the PIEE Solicitation Module website at: https://piee.eb.mil/sol/xhtml/unauth/index.xhtml via Solicitation Number Search W912HZ22R0007.

It shall be the contractor's responsibility to check the websites for any amendments. The offeror shall submit in the proposal all requested information specified in this solicitation. There will be no public opening of the proposals received as a result of this solicitation.

The vendors shall access the solicitation solely within PIEE and from within PIEE Solicitation Module, search and download a solicitation's documents. Vendors shall not use SAM.gov to access the solicitation.

A list of interested vendors (potential offerors and subcontractors) is available on the PIEE Solicitation Module (registration required) at: https://piee.eb.mil/sol/xhtml/unauth/index.xhtml via Solicitation number Search W912HZ22R0007.

d. Offeror's Questions and Comments. Technical inquiries and questions relating to this solicitation are to be submitted via Bidder Inquiry in ProjNet at (https://www.projnet.org) no later than (NLT) 7 calendar days prior to the proposal due date, and any new inquiries or questions submitted after that date will not be answered. (Note: Throughout the 30 calendar days before the solicitation due date, "Offeror/Bidder Inquiries" will be answered in a reasonable time). To submit and review inquiry items, prospective vendors will need to use the Bidder Inquiry Key presented below and follow the instructions listed below the key for access. A prospective vendor who submits a comment /question will receive an acknowledgement of their comment/question via email, followed by an answer to the comment/question after it has been processed by our technical team.

All timely questions and approved answers will be made available through ProjNet. Approved answers to all timely questions will also be posted as an amendment to the solicitation in the form of a report generated from ProjNet as soon as the comment/question entering period is over and all answers are finalized.

The Solicitation Number is: W912HZ-22-R-0007
The Bidder Inquiry Key is: **NMAD69-S5TI2F**

Specific Instructions for ProjNet Bid Inquiry Access:

1. From the ProjNet home page linked above, click on **Quick Add** on the upper right side of the screen.
2. Identify the Agency. This should be marked as USACE.
3. Key. Enter the **Bidder Inquiry Key** listed above.
4. Email. Enter the email address you would like to use for communication.
5. Click Continue. A page will then open saying that a user account was not found and will ask you to create one using the provided form.
6. Enter your First Name, Last Name, Company, City, State, Phone, Email, Secret Question, Secret Answer, and Time Zone. Make sure to remember your Secret Question and Answer as they will be used from this point on to access the ProjNet system.
7. Click Add User. Once this is completed you are now registered within ProjNet and are currently logged into the system.

Specific Instructions for Future ProjNet Bid Inquiry Access:

1. For future access to ProjNet, you will not be emailed any type of password. You will utilize your Secret Question and Secret Answer to log in.
2. From the ProjNet home page linked above, click on **Quick Add** on the upper right side of the screen.
3. Identify the Agency. This should be marked as **USACE**.
4. Key. Enter the **Bidder Inquiry Key** listed above.
5. Email. Enter the email address you used to register previously in ProjNet.
6. Click Continue. A page will then open asking you to enter the answer to your Secret Question.
7. Enter your Secret Answer and click Login. Once this is completed you are now logged into the system.

e. NAICS/Small Business Size Standard. The North American Industry Classification System (NAICS) Code for this acquisition is 541519, Other Computer Related Services. The small business size standard is $30,000,000. It is the offeror's responsibility to ensure that its classification data in the System for Award Management (SAM) website is correct and current.

f. Proposal Expense and Pre-Contract Costs. This Request for Proposal (RFP) does not commit the Government to pay, as a direct charge, any costs incurred in the preparation and submission of a proposal.

g. Pre-Proposal Conference. The Government plans to hold a pre-proposal conference. Specific information will be provided via amendment to the solicitation.

h. Accuracy in Proposals. Proposals must set forth full, accurate, and complete information as required by this RFP, (including attachments). The penalty for making false statements is prescribed in 18 U.S.C. 1001.

i. Submitting Proposals. Each volume of the proposal shall be electronically submitted via the PIEE Solicitation Module website at: https://piee.eb.mil/sol/xhtml/unauth/index.xhtml. Search via Solicitation Number Search W912HZ22R0007. In order to submit a Proposal, Vendors must register in the PIEE System and must have Proposal Manager Role established. Additional information regarding Proposal Manager Functions and Posting Offers can be found at https://pieetraining.eb.mil/wbt/xhtml/wbt/sol/solicitation/proposals.xhtml. OFFERORS MUST SUBMIT PROPOSALS TO BE RECEIVED NO LATER THAN THE DATE AND TIME STATED ON THE STANDARD FORM (SF) 1449 OR SUBSEQUENT SOLICITATION AMENDMENT.

QUESTIONS CONCERNING PROPOSAL RECEIPT CAN BE DIRECTED TO THE CONTRACT SPECIALIST / CONTRACTING OFFICER LISTED IN THE SOLICITATION. FOLLOW THE PROPOSAL FORMAT OUTLINED IN SECTION 2.0.

In the unlikely event the PIEE system is not operational, experiences technical difficulties, or a Contractor is temporarily unable to access or use the system, the Contractor shall immediately notify the Contracting Officer. This Notification must occur prior to the proposal submission deadline. Contractor notification shall be in writing and may be in conjunction with verbal notification, but verbal notification alone shall not be sufficient.

Any portion of the proposal that is changed (as a result of negotiations or proposal revisions) should be annotated and dated. Each volume shall be clearly labeled with its Title and a copy number (e.g., copy 1 of 5).

Each paragraph should be single spaced and shall be separated by at least one blank line. A standard, 12-point minimum font size applies. Arial or New Times Roman fonts are required. Tables and illustrations may use a reduced font size no less than 8-point and may be produced in landscape mode.

j. Oral Presentations. Oral presentations will not be utilized in conjunction with this solicitation. However, the Government reserves the right to conduct oral discussions as necessary with offerors determined to be in the competitive range.

k. Facsimile Use. Facsimile proposals or modifications will not be accepted.

l. Joint Venture and LLC Proposal Requirements. When proposing as a joint venture, all members of the joint venture shall sign the SF 1449 unless a written agreement by the joint venture is furnished with the proposal designating one firm with the authority to bind the other member(s) of the joint venture. In addition, a copy of the joint venture agreement shall be submitted with the proposal. Failure to comply with the foregoing requirements may eliminate the proposal from further consideration. If this is an 8(a) joint venture, the offeror shall ensure that it complies with the applicable requirements of 13 CFR Part 124 and 13 CFR Part 126, respectively. When proposing as a Limited Liability Company (LLC), a member authorized to bind the LLC shall sign the SF 1449. A copy of the LLC Certificate of Organization, Articles of Organization and the Operating Agreement shall be submitted with the proposal.

m. The following volumes of material shall be submitted:

Volume	Title	Digital Copies	Maximum Pages
I	Factor 1 – Technical **(AM #0002)** (Summary Section is not considered in the maximum page count) **(AM #0002)**		
	Tab 1, Sub-Factor 1 – Top Secret Facility Clearance	1	No page limit
	Tab 2 Sub-Factor 2 – Technical Approach	1	20
	Tab 3 Sub-Factor 3 - Management Approach	1	10
	Tab 4, Sub-Factor 4 – Transition Plan	1	2
II	Factor 2 – **(AM #0002)** Past Performance (PPQs, CPARS, ~~and Specialized Experience~~ Letters of Commitment (Attachment 4), performance recognition documents, and explanation of adverse past performance information are not considered in the page count) **(AM #0002)**	1	~~3~~20 **(AM #0002)**
III	Factor 3 - Price	1	No page limit

IV	PRE-AWARD INFORMATION_- Cover Letter (if applicable), Solicitation / Amendments, Offer and Award Documents, Certifications / Representations and other required pre-award information.	1	No page limit

NOTE: Pages that exceed the required page limitations will not be evaluated. Additional pages over the maximum allowed will be removed or not read and will not be evaluated by the Government.

2. PROPOSAL FILES

a. Proposal Format. Unless stated otherwise, proposal materials shall be in 8 ½" x 11" format, using 12 point minimum font size, using Arial or New Times Roman fonts only. Each volume will contain a Title Sheet for ready identification of the proposal including the offerors CAGE and DUNS/Unique ID numbers, a first page in accordance with FAR 52.215-1(c) (2) (i)-(v) and a full table of contents. Within each volume, it is recommended that the proposal information be presented in the same relative format as the submission requirements are listed, and the paragraph number from the submission requirements be used in the heading for the respective section/paragraph where the information is being provided.

(i) A Table of Contents should be created using the Table of Content feature in MS Word. MS Word (doc) files shall use the following page setup parameters:

Margins – Top, Bottom, Left, Right – 1"
Gutter – 0"
From Edge – Header, Footer 0.5"
Page Size, Width – 8.5"
Page Size, Height – 11"

(ii) The prime, consortium, or joint venture's name, address, a signature of the official that can bind the firm and a telephone number and email address shall appear in the lower left corner of the title page of any document/volume to be evaluated.

(iii) The offerors shall label and tab their proposal consistent with the solicitation format index below. Volume number, section/tab number, page number and date submitted shall appear in the bottom right corner of each page (along with the revision number for the amended page, if necessary). Page numbering shall re-start with each Tab. The Government will not evaluate any material exceeding the page limitations stated in the RFP. Pages will be counted as follows: one side of the paper is one page; information on both the back and front of one sheet of paper will be counted as two pages. Pages furnished for organizational purposes only, such as a "Table of Contents" or divider tabs, are not included in the page limitation.

(iv) Do not include exceptions to the terms and conditions of the solicitation in either the technical or price portions of the proposal. Should the offer include any standard company terms and conditions that conflict with the terms and conditions of the solicitation, the offer may be determined ineligible for award.

b. Acknowledgement of Amendments. Receipt of ALL Amendments must be acknowledged with the return of all applicable SF30s issued in response to the RFP. If uncertain as to the number of amendments issued, please contact via email at kevin.j.culley@usace.army.mil or melissa.k.lynn@usace.army.mil. Failure to acknowledge and return amendments with the submitted proposal may result in rejection of the offer.

c. Content Requirement. All information shall be confined to the appropriate file. The offeror shall confine submissions to essential matters, sufficient to define the proposal in a concise manner, to permit a complete and accurate evaluation of each proposal. Each file of the proposal shall consist of a Table of Contents, Summary Section, and the Narrative discussion. The Summary Section shall contain a brief abstract of the file. **(AM #0002)** The Summary Section of Volume I will not count toward the maximum page count. The Summary Table of CSSP Experience of Volume II shall count toward the maximum page count. **(AM #0002)** Proprietary information shall be clearly marked. The following shall be included in the Narrative discussion:

(i) VOLUME I – Factor 1 - Technical. The volume shall be organized into the following sections:

(1) Volume 1 - Tab 1 – Subfactor 1. This subfactor evaluates the offeror's **Top Secret Facility Clearance.**

Subfactor 1 Submission Requirements. As part of the offeror's proposal, the offeror shall complete Block 6 and submit the attached DD254 (Attachment 1) with the appropriate contractor information. Any proposed subcontractor that will execute any secured portion of this contract must also be included on line 7 of the DD254 as part of their submission and must possess the applicable security clearance level to the work that they will execute under this contract. **(AM #0002)** Joint Venture (JV) offerors shall comply with the 2020 NDAA and 13 C.F.R. Section 121.103(h)(4) in meeting these requirements. **(AM #0002)** All facility security requirements for the prime and any subcontractor must be met at the time of proposal submission.

(2) Volume 1 – Tab 2 - Subfactor 2. This subfactor evaluates the offeror's **Technical Approach.**

Subfactor 2 Submission Requirements. The offeror shall demonstrate its capability to provide a sound technical approach to meet all of the requirements of the PWS and satisfy the needs outlined for each specific functional area.

The approach shall describe in detail the actual methodology that will be employed for accomplishing/satisfying all of the requirements specified in the solicitation to include a discussion on how the offeror will assess the technical and contractual requirements of the PWS and determine the most effective allocation of effort among prime and any proposed subcontractor/team members. Do not merely reiterate the objectives or reformulate the requirements specified in the solicitation. The proposal should not simply rephrase or restate the Government's requirements or the requirements of the PWS but rather shall provide a narrative and rationale demonstrating the offeror understands, is able to meet, and intends to meet these requirements. Offerors shall assume that the Government has no prior knowledge of the offeror's capabilities and experience and will base its evaluation only on the information presented in the offeror's proposal. Responses shall not be a restatement of the requirement.

The offeror shall organize their response in two (2) separate sections:

1. Discussion of their technical approach to performing the major requirements of the PWS: Sections 3.1 through 3.7 (inclusive)
2. Discussion of their technical approach for the following:
    - Developing an Insider Threat program for a DoD CSSP in accordance with DODD 5205.16
    - Maintaining a robust and consistent security environment in accordance with (IAW) current Evaluator Scoring Metrics (ESM) and DODI 8530.1
    - Coordinating and preparing for DoD evaluations and inspections

Executing DCO requirements, following specific DoD Cyber Incident Handling Program requirements (i.e., CJCSM 6510.01B) in a multi-Service/Agency environment, and an understanding of DoD Areas of Operation (AOs) and how they are used to organize the DODIN.

(3) Volume 1 - Tab 3 – Subfactor 3. This sub-factor evaluates the offeror's **Management Approach.**

Subfactor 3 Submission Requirements. The offeror shall demonstrate its capability to provide a sound management approach to meet all of the requirements of the PWS and satisfy the needs outlined for each specific functional area as well as the overall management of the contract.

The management approach and staffing plan shall fully describe the structure of the proposed organization/team (including subcontractors/team members) that will be utilized to accomplish the requirements identified in the PWS. Describe how this proposed team fits into the overall corporate structure and the reporting and review relationship with corporate management. Delineate responsibilities (of the prime and subcontractors), management of Key

Subcontractors, lines of authority, and spans of control, as well as how the offeror will control the flow of information and communications among team members, customers, the COR and the Contracting Officer. For key Subcontractors (defined as any subcontractor or teaming partner that will perform more than 20% of the work or 20% of the total contract value), provide a detailed description of all teaming/subcontracting arrangement. Identified Key Subcontractors must complete the Letter of Commitment. Letters of Commitment do not count against the page limitation for this section. Also, describe how the Key Subcontractors will be managed and how risk will be mitigated to ensure successful performance of the PWS requirements. The discussion shall include the processes that will be employed to maintain privity of contract restrictions while, at the same time, efficiently conveying Government technical requirements to team members/subcontractors, implementing changes in technical direction, monitoring/measuring their performance, and ensuring that all task objectives are achieved. Discuss any unique organizational business practices or management of subcontractors that will be implemented to facilitate the successful execution of the HPCMP CSSP. Do not merely reiterate the objectives or reformulate the requirements specified in the solicitation. The proposal should not simply rephrase or restate the Government's requirements or the requirements of the PWS but rather shall provide a narrative and rationale demonstrating the offeror understands, is able to meet, and intend the meet these requirements. Offerors shall assume that the Government has no prior knowledge of the offeror's capabilities and experience and will base its evaluation only on the information presented in the offeror's proposal. Responses shall not be a restatement of the requirement.

The offeror shall organize their response in four (4) separate sections:

1. The offeror's overall management approach
2. The offeror's proposed staffing plan for each of the PWS major requirements (PWS Sections 3.1 through 3.7, inclusive). This must include the offeror's proposed quantity of hours and work location (named site or virtual) for each labor category being proposed for each PWS section.
3. A discussion of the offeror's personnel fill/recruitment/retention methodology.
4. A discussion of the offeror's proposed Key Personnel. Proposals shall provide adequate and clear information that establishes that the proposed Key Personnel possess qualifications, experience, and capabilities that meet or exceed the applicable minimum qualifications established in the PWS to effectively perform the requirements of the contract.

(4) Volume 1 - Tab 4 – Subfactor 4. This sub-factor evaluates the offeror's **Transition Plan.**

Subfactor 4 Submission Requirements. The transition/phase in plan submittal shall address the offeror's approach to effectively and efficiently transition/phase-in resources and personnel onto the contract and ensure full continuity of HPCMP CSSP support on the required performance start date of the contract. The plan shall address the Offeror's approach to ensure a seamless transition with outgoing contractors on efforts requiring continued support. This plan shall include transition period length and key activities. A transition period is intended to provide an orderly transfer of support responsibilities from the incumbent contractor to the contractor selected for this effort. **(AM #0005)** Transition shall be for a period of 90 days prior to full performance of the contract. **(AM #0005)**

All aspects of the transition planning phase shall be addressed to include, but not limited to:

- How the contractor will be organized structurally during the transition (phase-in) period.
- What the contractor identifies as their critical learning and action processes.
- Schedule for transition and integration.
- Upon end of transition period, utilize a workforce capable of immediately accomplishing the mission of the CSSP contract requirements.

(ii) VOLUME II – Factor 2 - Past Performance.

Factor 2 Submission Requirements. The Proposal must include no more than three (3) projects of similar size, scope and complexity representing the offeror's relevant Past Performance using the attached Past Performance Questionnaire (PPQ) form performed within the past three years. In responding to this factor, the objective is to demonstrate to the evaluators that the offeror clearly has the capability to successfully complete all

aspects of the requirements by explaining in detail how the provided demonstrated past performance experiences are similar to the work described in the solicitation. Projects can be task orders or site specific/stand-alone contracts. Do not list an IDIQ base contract with multiple task orders as a project example, but instead list the relevant IDIQ task order issued for a specific project/site. Projects may have been performed for Federal, State/local Government or private clients.

A maximum of three (3) projects will be evaluated. If an offeror disregards these instructions and submits more than three projects, only the first three projects will be evaluated. Offerors shall describe each project with enough detail to ensure that the Government can meaningfully assess the projects against the evaluation criteria described in the RFP.

Relevant Past Performance is defined as past performance on projects that show the contractor's ability to execute the same/similar in scope/size/complexity of the requirements to the CSSP specifications identified in this solicitation.

- Provide a Summary Table of CSSP Experience, (page limitation is one (1) 8 1/2" x 11" page), to address demonstrated past performance experience of the three projects included in the proposal.

For each project submitted, the offeror shall provide:

- Project description and information using "Offeror Past Performance Project Experience Form" (Attachment 2). The offeror must address all items included on Attachment 2 (no more than two (2) pages per project). The "Offeror Past Performance Project Experience Form" may also be used for key subcontractor experience if included as part of the team. Offerors may identify state and local government and private contracts that are similar to the requirements of this solicitation.
- Experience in the narrative should include but is not limited to:
  - Performing 24/7/365 defensive cybersecurity operations for the DoD
  - Administering systems/network infrastructure
  - Administering DoD's ACAS, HBSS, and Tanium servers
- Include performance recognition documents received within the last five (5) years such as awards, award fee determinations, customer letters of commendation, and any other forms of performance recognition.
- If a completed Contractor Performance Assessment Reporting System (CPARS) evaluation is available, submit it with the proposal.
- If there is not a completed CPARS evaluation, submit a completed Past Performance Questionnaire (PPQ) (Attachment 3) for the project. Offerors are advised to ensure correct phone numbers and email addresses are provided for the Client point of contact. (Do not submit a PPQ when a completed CPARS evaluation is available).
- If the Offeror is unable to obtain a completed PPQ from a client for a project(s) before proposal closing date, the Offeror should complete and submit with proposal the first page of the PPQ, Offerors should follow up with clients/references to ensure timely submittal of questionnaires. If the client requests, questionnaires may be submitted directly to the Government's point of contact, Melissa K. Lynn via email at melissa.k.lynn@usace.army.mil prior to proposal closing date. Offerors shall instruct the clients to refer to the solicitation number in the subject line.
- PPQs are source selection materials. All successfully submitted PPQs will receive an email confirmation upon receipt. If the offeror does not receive the confirmation, it is the offeror's responsibility to follow up to ensure the Government has received the information.
- Offerors shall not incorporate by reference into their proposal PPQs or CPARS previously submitted for other procurements. However, this does not preclude the Government from utilizing previously submitted PPQ information in the past performance evaluation.
- Offerors may provide explanation on problems encountered on past projects and the corrective actions taken by the offeror.

Failure to provide sufficient detail explaining how the proposed provided experience is similar to the work described in the solicitation may be noted as a deficiency. The offeror should clearly demonstrate it has the capability to successfully complete the project. Offerors should presume that the technical evaluators are unfamiliar with the provided demonstrated experience and are responsible for providing detailed explanations regarding the work and how said work is similar to that described in the solicitation.

In addition to the above, the Government may review any other sources of information for evaluating past performance. Other sources may include, but are not limited to, past performance information retrieved through the CPARS, using all CAGE/DUNS (and Unique Entity Identifier (UEI) numbers of team members (partnership, joint venture, teaming arrangement, or parent company/subsidiary/affiliate) identified in the offeror's proposal, inquiries of owner representative(s), Federal Awardee Performance and Integrity Information System (FAPIIS), Electronic Subcontract Reporting System (eSRS), telephone interviews with organizations familiar with the offeror's performance, Government personnel with personal knowledge of the offeror's performance capability, and any other known sources not provided by the offeror.

While the Government may elect to consider data from other sources, the burden of providing detailed, current, accurate, and complete past performance information rests with the offeror.

While the Government will consider past performance experience information on relevant projects performed for state and local Governments, as well as in the commercial sector, past performance experience conducted within DOD/USACE will receive greater consideration when assigning a past performance relevancy and confidence assessment rating than those for work performed for organizations other than the DoD.

Offerors shall ensure the PPQs provided contain contract name/title; client point-of- contact(s) with confirmed correct phone numbers and email addresses; geographic location of contract; date of contract periods of performance; final US dollar contract value; description of the contract including scope, and description of the offeror's involvement with the performance of the contract.

If submitting relevant experience under a previous business relationship, clearly describe the offeror's role on the past experience project. An offeror may receive credit for relevant experience under a previous business arrangement (joint venture for example) only if the offeror demonstrates that their role on the submitted project is relevant to their role on this project.

If any portion of work provided as demonstrated experience is from a parent company, clearly identify that work as it relates to this project. Using Attachment 4, Letter of Commitment, from the parent company clearly stating that they will provide their expertise and support, as necessary, as it relates to the portion of work used as demonstrated experience for this project. Failure to include a letter of commitment will be noted as a deficiency.

If any portion of work provided as demonstrated experience is subcontracted, clearly identify that work as such and provide the required experience of that subcontractor as it relates to the work the subcontractor will be performing on this project. Using Attachment 4 provide a letter of commitment from the proposed subcontractor. Failure to include a letter of commitment will be noted as a deficiency.

(iii) VOLUME III – Factor 3 - Price.

Factor 3 Submission Requirements. Proposals received without a completed Price Proposal Template and other required documentation identified below will be considered non-conforming and may not be considered for contract award. All prices should be based on the PWS requirements. Service Contract Act (SCA) exemption: As the labor categories of this requirement are considered "Executive, Administrative or Professional", offerors shall be responsible for ensuring compliance with the SCA for other applicable Labor Categories.

Price Proposal shall include:

(1) Attachment 5 Price Proposal Template - Offeror shall complete the provided Price Proposal Template using the provided Excel spreadsheet. Offeror shall submit an Excel version of their completed Price with their proposal.
(2) Attachment 5 Price Proposal Template – Offeror shall provide a PDF version of all tabs of Price Proposal Template and submit with their proposal.
(3) Pricing Assumptions – Offerors shall provide an itemized detailed summary of all pricing assumptions with their proposal.
(4) Submit the Proposal Data Sheet (Attachment 6)
(5) If requested, submit Data Other than Certified Cost or Pricing Data in accordance with FAR 52.215-20

Other Price Proposal Information:

Attachment 5 Price Proposal Template Instructions:

Offerors shall complete the following information on Attachment 5 Price Proposal Template. Note: Sections highlighted in gray are protected and not editable by the offerors. Submission of a version other than the RFP's Attachment 5 Price Proposal Template will be considered non-conforming and deem the price proposal unacceptable.

STEP 1: Complete the TAB "Proposed Labor Categories/Rates".

Offeror shall use this tab to develop and build the various labor categories and hourly labor rates that will be used to establish the overall monthly rate for Contract Line Item Numbers (CLINs) 0001/1001/2001/3001/4001 of the contract. Offeror will rename the cells in column A to corresponding labor categories/title and input loaded labor rates for the base year, option year 1, option year 2, option year 3, and option year 4. These labor categories will represent the specific labor categories needed to complete the PWS tasks.

In addition, the labor rates for this tab shall be all inclusive of wages, overhead (as applicable), general and administrative expenses, profit, material handling, and subcontractor/ subcontractor handling costs. The rates on this tab shall be based on the hours of operation required in PWS 2.6.2 and shall also include the estimated costs for on-call support outside of core hours as described in PWS section 3 and **(AM #0005)** ~~phase-in/~~phase-out costs as detailed below: **(AM #0005)**

- Call-in hours/time: Historical data of known past call-in hours have been provided as part of the Attachment 5 Price Proposal Template, Tab "Historical Labor Hour Info" for proposal consideration. Offerors are cautioned that no separate payment of hours due to the call-in of on-call staff during non-core hours will be made or considered by the Contracting Officer Representative or the Contracting Officer. Offerors are to include the estimated costs of call-in hours based on the provided historical data and estimates into their loaded rates of CLINs 0001/1001/2001/3001/4001 on the **TAB "Proposed Labor Categories/Rates".**
- **(AM #0005)** ~~Phase-in/~~Phase-out: Any ~~phase-in~~/phase-out costs shall be built into the overall costs of the monthly rate of CLINs 0001/1001/2001/3001/4001. No additional costs for ~~phase-in/~~phase-out will be reviewed for future consideration. These costs shall be included in the loaded rates on the TAB "Proposed Labor Categories/Rates". **(AM #0005)**

STEP 2: Complete the TAB "Proposed Labor Mix and Hours"

Offerors shall use the labor categories and labor rates created from the **TAB "Proposed Labor Categories/Rates"** to develop their labor mix and hours for their proposed monthly contract rate for PWS Tasks 3.1-3.7. The offeror will choose the applicable labor category from the drop-down list in column A, for each of the assigned PWS tasks. The labor rates for the base and all options will copy from the **TAB "Proposed Labor Categories/Rates"**. In addition, the offeror will need to assign the number of yearly hours for that assigned labor category in column B, based on a rate of 1,920 hours per Full Time Equivalent (FTE). For informational purposes only, **TAB "Historical Labor Hour Info"** is provided as a reference to past number of hours by PWS task.

Upon insertion of all labor categories/labor rates and all hours, the total calculation for the yearly FFP contract value for labor will calculate on the **TAB "Roll-up"**, CLINs 0001/1001/2001/3001/4001/Extension. The **TAB "Details"** will provide a calculation for the individual Task Levels 3.1-3.7. These yearly totals on the **TAB "Roll-Up"** will be divided by 12, providing a FFP monthly contract rate.

For evaluation purposes, the highest labor rate in each PWS task 3.1-3.7 will be used to calculate the overall total evaluated price of the surge CLINs. The **TAB "Surge Labor Totals"** will pull the "MAX" value (highest labor rate) of each task (by year/CLIN) and calculate those times the number of estimated hours for that task to derive a value for that CLIN. The spreadsheet will calculate a total for the Base Year and each Option Year using the same calculation method. These values will then copy into the **TAB "Roll-Up"** on CLINs 0002/1002/2002/3002/4002/5002(Extension). These values will be included in the calculation of the total evaluated price for all contract CLINs. **TAB "Surge Labor Totals"** is protected and not editable by the offerors.

STEP 3: Update the ODC G&A Percentage/Dollars on TAB "Roll-Up"

Other Direct Cost Related Information – The offeror may propose a fixed percentage G&A to be applied to other direct costs (ODC) (travel, training and OLM) when processing modifications for known requirements for those line items. Profit shall not be allowed on any action for ODC requirements. The proposed G&A percentage shall be fixed for the duration of the contract. Offeror shall include the proposed G&A percentage rate on **TAB "Roll-Up",** Line 12 - ODC G&A Percentage/Dollars. The proposed G&A dollars will automatically be calculated based on the fixed estimated ODC CLIN amounts and the proposed percentage rate with the total G&A dollars being included in the total evaluated proposed price. This dollar value will be used for evaluation purposes of the total evaluated price only. If the offeror intends to propose a rate of 0% for its G&A, it will need to be noted specifically on the spreadsheet in cell A26 to clarify its intent.

For evaluation purposes, CLINs for **Travel** (all years), **Training** (all years) and **Order Level Materials (OLM)** (all years) have been provided as fixed estimated values and will not be adjusted for the offeror's proposal. These values are protected and not editable by the offerors.

(AM #0005) STEP 4: Provide a rate for 90 day Transition period prior to full performance of contract on CLIN 0006 of Attachment 5, Price Proposal Template. **(AM #0005)**

Cost or Pricing Information Requirements – In accordance with FAR 15.402, 15.403-1(b) and 15.403-3(a), "information other than cost or pricing data" may be required to support price reasonableness. If, after receipt of proposals, the Contracting Officer determines that there is insufficient information available to determine the reasonableness of the proposed pricing, the Offeror shall be required to submit additional information other than cost or pricing data. If, during the evaluation process, the Contracting Officer determines that adequate competition no longer exists, then cost or pricing data may be required to determine a fair and reasonable price.

Do not complete RFP/Solicitation Section B with pricing information. All pricing information will be contained in the Attachment 5 Price Proposal Template.

This solicitation does not commit the Government to pay any costs incurred in the preparation and submission of offeror's proposal(s) or in making any necessary studies for the preparation thereof, or for any visit the Contracting Officer may request for the purpose of clarification of the proposal or for preparation for negotiations.

Paragraph (c) of FAR 52.212-1 is replaced as follows:

(AM #0005) Period for Acceptance of Proposals/Offers. The suppliers/offeror agrees to hold the prices in its proposal firm for 180 calendar days from the date specified for receipt of proposals/offers **(AM #0005).**

Paragraph (f) of FAR 52.212-1 is supplemented as follows:

Late submissions, modifications, revisions, and withdrawals of offers: Offeror is responsible for submitting offers, and any modifications, revisions, or withdrawals, so as to reach the Government office designated in the solicitation

by the time specified in the solicitation IAW FAR 15.208, Submission, Modification, Revision, and Withdrawal of Proposals. The time specified in the solicitation for receipt of offers is local time, Central Standard Time (CST), Vicksburg, Mississippi.

Other Price Proposal Information:

(1) Compliance. Failure to comply with the RFP requirements for cost and price information may result in an adverse assessment of an offeror's proposal and reduce or eliminate its chance of being selected for award. Offerors shall ensure that the information presented in this volume is consistent and correlates with the information contained in the other proposal volumes. Also, the Offeror shall ensure that the information submitted in this volume is consistent with and fully supports the amounts set forth in the solicitation.

(2) General Instructions. In accordance with Federal Acquisition Regulation (FAR) 15.402 and 15.403-1, certified cost or pricing data are not required based on the fact that adequate competition is expected for this procurement. Information other than certified cost or pricing data may be provided in contractor format providing that sufficient information is made available. Information submitted shall be prepared following the instruction in FAR 15.403-5. If after receipt of proposals the Contracting Officer determines that there is insufficient information available to determine price reasonableness and none of the exceptions at FAR 15.403-1 apply, the Offeror may be required to submit cost or pricing data. Additionally, in the event that adequate competition is not obtained, the Contracting Officer may incorporate FAR 52.215-20 entitled, "Requirements for Cost or Pricing Data or Information Other Than Cost or Pricing Data," into the solicitation and request a Certificate of Current Cost or Pricing Data. There are no page limitations for this volume. Proposal information included in this volume which is not directly related to Cost will be disregarded.

(iv) VOLUME IV – PRE-AWARD INFORMATION

Pre-Award Information Submission Requirements. Solicitation/RFP, all signed amendments, offer and pre-award information.

Submit this information for the Contracting Officer's determination of Offeror responsibility, which includes, but is not limited to the following:

Joint Venture agreement or Limited Liability Company Certificate of Organization, Articles of Organization and Operating Agreement, if applicable. These documents must clearly identify the individual(s) authorized to bind the company.

A Copy of Firm's Annual Financial Statement(s) for the past three years (or for the period it has been in business, if less than three years).

A Copy of Firm's current credit report(s) (include Name, address and telephone numbers of two credit/trade references).

A list of present commitments, including the dollar value thereof, and name of the organization under which the work is being performed. Include names and telephone numbers of personnel within each organization who are familiar with the prospective contractor's performance.

A certified statement listing: (1) each contract awarded within the preceding three-month period exceeding $1,000,000.00 in value with a brief description of the contract; and (2) each contract awarded within the preceding three-year period not already physically completed and exceeding $5,000,000.00 in value with a brief description of the contract. If the prospective contractor is a joint venture, each joint venture member will be required to submit the above defined certification

Completed Representations and Certifications by filling out FAR 52.212-3 Offeror Representations and Certifications—Commercial Products and Commercial Services. List any changes to Online Representations and Certifications. Provide any certifications where contractor indicated in the online representations and certifications that the certification would be provided with specific offer.

Additional information required for responsibility determination:

1. List of pending lawsuits or unsatisfied judgments against your firm, the nature of same and Court were filed or adjudicated. Lawsuits or judgments where full payment will be made or are covered by your insurance are not to be included.

2. Number of years the firm has been in business

3. An explanation of the firm's capability to obtain sufficient financial resources to perform work required under any resulting contract from this solicitation.

(End of Summary of Changes)

Controlled Unclassified Information (CUI) Only

Bid Inquiry Contractor Report
All Inquiries Resolved Between 17-Nov-22 and 14-Dec-22

Project: HPCMP - CSSP **Review**: RFP Question and Comments (*00001*)
(sorted by CommentID)
Displaying 18 inquiries.

Id	Discipline	Sheet	Detail	Spec
9995592	Cybersecurity	Statement of Work	Technology	Statement of Work
Comment Classification: **Controlled Unclassified Information (CUI)** Please provide the technologies and tools you use today. On: Nov 17 2022.				
	Government Response. . Tools and technologies in use for the HPCMP CSSP are comprised of commercially available software commonly in use around the United States and custom software in use for the U.S. DoD, U.S. Army, USACE, and HPCMP. No comprehensive, complete list is available, as such tools change based on need. On: Nov 21 2022			
	Current Request Status: **Request Closed**			
Information for this report is procurement sensitive.				
9996431	Inform Sys Comm	Section 3.1 Program Manager	Table 2: Minimum Clearance Requirements	Statement of Work
Comment Classification: **Controlled Unclassified Information (CUI)** Please specify the clearance required for the Program Manager. Under Table 2: Minimum Security Requirements, the PM clearance is not specified. Under Section 3.1, the PM is required to "Be intimately aware of all personnel's job duties and expectations." On: Nov 18 2022.				
	Government Response. . PM would be required to have no less than a secret clearance. On: Nov 30 2022			
	Current Request Status: **Request Closed**			
Information for this report is procurement sensitive.				
9999209	Inform Sys Comm	Page 10 and Attachment 5	Historical Information	2.6.2 Hours of Operation
Comment Classification: **Controlled Unclassified Information (CUI)** The government only provided an on-call hours estimate for Section 3.5 Infrastructure Services (20-25 hrs/mon). The incumbent will have this historical experience information for on-call hours which provides a competitive advantage to them. To level the playing field, can the government either: 1. Provide the incumbent's on-call hours historical experience for the other task areas? OR 2. Provide a set number of hours (plug number) for all vendors to use for the on-call support? On: Nov 21 2022.				
	Government Response. . The information requested has been provided in the historical data tab of the Price Template. Each offeror is responsible for establishing a pricing model to cover its risk in this area given the information provided in the RFP. On: Nov 30 2022			
	Current Request Status: **Request Closed**			
Information for this report is procurement sensitive.				
10000085	Contracting			2.1
Comment Classification: **Controlled Unclassified Information (CUI)** Is there a copy of the DRAFT DD Form 254 available? If so, could you provide the document? On: Nov 21 2022.				
	Government Response. . Attachment 1 of the initial RFP posting is the Draft DD254. On: Nov 30 2022			
	Current Request Status: **Request Closed**			
Information for this report is procurement sensitive.				
10000089	Contracting			3.6
Comment Classification: **Controlled Unclassified Information (CUI)**				

What are the projected award and start dates?

On: Nov 21 2022.

	Government Response. . Award is anticipated to be made by 30 June 2023 with a 90-day transition period. An amendment will be posted to include a standalone CLIN for this transition period for pricing and evaluation purposes. On: Dec 12 2022
	Current Request Status: **Request Closed**

Information for this report is procurement sensitive.

10000091	Cost Engineering			2.6.1

Comment Classification: **Controlled Unclassified Information (CUI)**

According to historical data we are tracking 47 employees, but on the RFP it appears there is space for 86 bodies. What is the objective staffing level?

On: Nov 21 2022.

	Government Response. . The information provided in the Price Template is historical data only. Offerors are expected to develop their own performance-based level of effort to support and execute the contract requirements. The number of spaces available in the Proposed Labor Categories and Labor Mix tab and Proposed Labor Mix and Hours tab provide the offeror the ability to create their own solution and labor mix to support each area of the contract. The Government will not provide an objective staffing level for this contract as it is a performance-based requirement. On: Nov 30 2022
	Current Request Status: **Request Closed**

Information for this report is procurement sensitive.

10000094	Contracting	Page 9		2.6.1

Comment Classification: **Controlled Unclassified Information (CUI)**

What are the total headcounts per position and location?

On: Nov 21 2022.

	Government Response. . The Government will not dictate these numbers, historical data is provided for guidance. On: Nov 30 2022
	Current Request Status: **Request Closed**

Information for this report is procurement sensitive.

10000101	Contracting			2.6.1

Comment Classification: **Controlled Unclassified Information (CUI)**

What are the work hours per year? In the RFP it states 1920 hours per employee, but 10.5 hour days for a number of positions.

On: Nov 21 2022.

	Government Response. . 1912 is the productive hour level used with the new Juneteenth holiday considered. The Proposed Labor Mix and Hours tab reflects the new number of hours. On: Nov 30 2022
	Current Request Status: **Request Closed**

Information for this report is procurement sensitive.

10000106	Contracting			2.6.1

Comment Classification: **Controlled Unclassified Information (CUI)**

Will there be any incumbent contractors that will be rolled over to our payroll? If so, do you have approximate headcount, positions, and locations?

On: Nov 21 2022.

	Government Response. . This is not something the Government will dictate. Employee retention from the current contractor will be in accordance with applicable laws, statutes and contract awardee. On: Nov 30 2022
	Current Request Status: **Request Closed**

Information for this report is procurement sensitive.

10000108	Cost Engineering			2.6.1

Comment Classification: **Controlled Unclassified Information (CUI)**

Is there relocation assistance funding within the cost model for the positions?

On: Nov 21 2022.

	Government Response. . The Government does not have a position on this as this will be up to the individual offeror to consider in their proposal. On: Nov 30 2022			
	Current Request Status: **Request Closed**			
Information for this report is procurement sensitive.				
10000109	Contracting			2.6.1
Comment Classification: **Controlled Unclassified Information (CUI)** As currently defined for remote positions, it mentions not providing internet or a phone, but will a government furnished laptop be provided? On: Nov 21 2022.				
	Government Response. . Government furnished laptop will be provided for remote positions. On: Nov 30 2022			
	Current Request Status: **Request Closed**			
Information for this report is procurement sensitive.				
10000114	Contracting			2.6.1
Comment Classification: **Controlled Unclassified Information (CUI)** As currently defined for remote positions, it mentions not providing internet or a phone, but will a government furnished laptop be provided? On: Nov 21 2022.				
	Government Response. . Same question as Inquiry ID 10000109. See response at Inquiry ID 10000109 for resolution. On: Nov 30 2022			
	Current Request Status: **Request Closed**			
Information for this report is procurement sensitive.				
10000115	Contracting	Page 10		2.6.2
Comment Classification: **Controlled Unclassified Information (CUI)** For on-site positions, is there a process to clear any contractor laptops to enter the area? On: Nov 21 2022.				
	Government Response. . Contractor laptops are permitted to enter the unclassified areas of the facilities, however they are not permitted to connect to the Government provided network. On: Nov 30 2022			
	Current Request Status: **Request Closed**			
Information for this report is procurement sensitive.				
10000117	Contracting			2.6.2
Comment Classification: **Controlled Unclassified Information (CUI)** There is a telework structure in place for unclassified work during facility closure. Could this be leveraged for scheduled telework while supporting Tasks 24/7/365? On: Nov 21 2022.				
	Government Response. . As stated in the PWS, situational teleworking is permissible with prior concurrence from the Government. On: Nov 30 2022			
	Current Request Status: **Request Closed**			
Information for this report is procurement sensitive.				
10000120	General			3.2
Comment Classification: **Controlled Unclassified Information (CUI)** What platform is utilized for the SIEM & EDR? What ticketing agent is currently utilized? On: Nov 21 2022.				
	Government Response. . HPCMP utilizes a GOTS solution for SIEM. HPCMP utilizes Endpoint Security Solution (ESS) for EDR. HPCMP utilizes Redmine as an internal ticketing system. On: Nov 30 2022			
	Current Request Status: **Request Closed**			
Information for this report is procurement sensitive.				
10000124	Cybersecurity			3.6
Comment Classification: **Controlled Unclassified Information (CUI)**				

Does the current program whitelist alerts? If so, to what extent? On: Nov 21 2022.				
	Government Response. . Yes, the HPCMP utilizes industry known best practices for defending the network terrain including whitelisting for all internet accessible VPNs and public facing websites. On: Nov 30 2022			
	Current Request Status: **Request Closed**			
Information for this report is procurement sensitive.				
10000126	Cybersecurity			3.5.4
Comment Classification: **Controlled Unclassified Information (CUI)** Is there currently a backlog of infrastructure tickets? We understand the response timelines, but is there a backlog at the moment? On: Nov 21 2022.				
	Government Response. . No, only ongoing projects. On: Nov 30 2022			
	Current Request Status: **Request Closed**			
Information for this report is procurement sensitive.				
10000130	General			2.6.1
Comment Classification: **Controlled Unclassified Information (CUI)** Is there additional detail on filled positions? Nature of work, scope, pay level and clearances by position? On: Nov 21 2022.				
	Government Response. . The Government will not provide any additional information on "filled postions" except that in the Historical Data tab of the Price template. The PWS defines the areas of work and tasks of this contract requirement. Table 2 of the PWS provides an overview of the minimum clearance requirements by functional area of the contract. On: Nov 30 2022			
	Current Request Status: **Request Closed**			
Information for this report is procurement sensitive.				

Report Complete

Attachment_5_Price Proposal Template - 20221215 -REV-3 Amend 0005

Use attached File