PERFORMANCE WORK STATEMENT

FOR

VULNERABILITY DISCLOSURE PROGRAM ENTERPRISE MANAGEMENT SYSTEM

22 September 2025

Contents

1.0 SECTION 1

1.1 GENERAL INFORMATION

The Department of Defense (DoD) Cyber Crime Center (DC3) Security office is responsible for managing a comprehensive Vulnerability Disclosure Program (VDP), and related services, to enhance the security of the DoD Information Network (DoDIN) and Defense Industrial Base (DIB) networks. This initiative, established in 2016 by the Secretary of Defense, leverages crowdsourced cybersecurity expertise to identify and remediate vulnerabilities, aligning with the DoD's defense-in-depth strategy, ISO 29147:2018 and ISO 30111 standards, and DoDI 8530.02, Cyber Incident Response

1.2 BACKGROUND

The DoD's computer networks and systems support the nation’s defense and are critical both for daily business operations and mission critical activities. Maintaining the security, confidentiality, availability, and integrity of DoD networks and systems is a matter of national security and requires the continuous identification and remediation of vulnerabilities that can be exploited by malicious cyber actors. As part of its responsibility to the public at large, DoD is constantly considering innovative and diverse approaches to meet this goal.

Crowdsourcing is a modern business practice that, as of 2010, the Federal Government has employed to obtain needed services, ideas, or content by soliciting contributions from a large group of people rather than from traditional employees or suppliers. Crowdsourcing incentivizes innovation in solving mission-centric problems. Remaining ahead of present and emerging cyber threats is a significant responsibility in any environment. For DoD, the responsibility is amplified as the repercussions associated with security failure are severe.

To support DoD's continual efforts to remain at the forefront of rapidly evolving technologies, and to maintain the highest levels of integrity and security required of its IT infrastructure, DoD has identified an emerging need to leverage a diverse pool of innovative information security researchers (herein referred to as "researchers") via crowdsourcing, for vulnerability discovery, coordination and disclosure activities

1.3 SCOPE

The Contractor will provide two enterprise management system licenses/subscriptions for DC3’s DoD VDP and DIB VDP which will facilitate collaboration, compliance, and management of a VDP within 10 business days of contract award **(Section 2, Deliverable 1)**.

The Contractor is responsible for providing a license/subscription to an enterprise management system for a VDP with the following components:

1.3.1 Enterprise-grade VDP platform license/subscription (2 – DoD VDP and DIB VDP)

1.3.2 Vulnerability Submission and Management Workflows as required **(Section 2, Deliverable 2)**

1.3.3 Inbox, Security Page, Disclosure Workflow, Community Engagement

1.3.4 Hacktivity, Leaderboard, Reputation System Integration Capabilities

1.3.5 Seamless integration with existing DC3 IT systems

1.3.6 Mediation Support

1.3.7 Tools and processes for effective vulnerability triage and resolution

1.3.8 Advanced analytics and custom reporting capabilities

1.3.9 A dedicated account team with customer support and customer success functions

1.3.10 250 crowdsourced vulnerability – bug tag and annual mailings as required **(Section 2, Deliverable 3).** The vendor will be responsible for the cost and labor of the shipping and logistics for DC3-provided, -designed and -manufactured items, used to recognize researchers for their annual contributions to the DC3 VDP.

1.4 TRANSITION IN

1.4.1 The contractor shall schedule, coordinate, and host a Kick-Off Meeting at the location approved by the Government **(Section 2, Deliverable 4)** within ten business days of Contract Award. The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the Contract. The meeting shall provide the opportunity to discuss technical and management issues. At a minimum, the attendees shall include Key contractor Personnel, representatives from government, and the AFDW/PKA Contracting Officer (CO) and COR.

1.4.2 The contractor shall, at least three business days prior to the Kick-Off Meeting, provide a Kick-Off Meeting Agenda **(Section 2, Deliverable 5)** for review and approval by the government prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

1.4.2.1 Points of Contact (POCs) for all parties.

1.4.2.2 Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government).

1.4.2.3 Staffing Plan and status.

1.4.2.4 Transition-In Plan and discussion.

1.4.3 Immediately following award, the contractor shall begin implementing its phased

Transition-In Plan (Section 2, Deliverable 6), provided as a part of the proposal. The contractor shall provide a status/progress update of its transition-in activities at the Kick-Off Meeting. The contractor shall notify the Government immediately of risks impacting transition

1.5 TRANSITION OUT

1.5.1 The contractor shall provide transition-out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming contractor at the expiration of the contract. The contractor shall provide a Transition-Out Plan within three months of Project Start (PS) **(Section 2, Deliverable 7)**. The Government will work with the contractor to finalize the Transition-Out Plan.

2.0 SECTION 2

2.1 SERVICE SUMMARY

The Contractor service requirements are summarized into performance objectives that relate directly to *mission essential items*. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement and will be assessed on an "Acceptable" or "Unacceptable" basis. These thresholds are critical to mission success. Program Management Reviews (PMR) will be conducted annually.

Table 1: Service Summary

Performance Objective	**PWS Para**	**Performance Threshold**	**Method of Surveillance**
SS – 1 Provide two enterprise-grade VDP platform licenses/subscriptions (DoD-VDP and DIB-VDP)	1.3	a) 95% of operational functions executed without issue b) License active and accessible 24/7 c) 100% compliance with license renewals and updates	100% Surveillance
SS – 2 Provide Vulnerability Submission and Management Workflows.	1.3.2	a) 100% of vulnerability submissions processed and acknowledged within 24 hours e) 95% of vulnerabilities triaged and routed for action within 5 business days	100% Surveillance
SS – 3 Provide inbox, Security Page, Disclosure Workflow, and Community Engagement	1.3.3	a) 95% uptime of inbox and disclosure workflows b) 90% satisfaction rating from annual community engagement surveys	Periodic Surveillance Survey Inspections

SS – 4 Provide Hacktivity Leaderboard, and Reputation System Integration Capabilities	1.3.4	a) 100% accuracy of researcher recognition data b) Leaderboard updated within 24 hours of validated submission	Periodic Surveillance Periodic Inspections
SS – 5 Ensure seamless integration with existing DC3 IT systems	1.3.5	a) 100% compliance with DC3 IT security interoperability, and accreditation standards b) No more that two integration failures annually	Periodic Surveillance
SS – 6 Provide mediation support	1.3.6	a) Mediation requests acknowledged within two business days b) 90% resolution rate within 15 business days	Customer Complaint Survey Inspections
SS – 7 Provide tools and processes for effective vulnerability triage and resolution	1.3.7	a) 95% of vulnerabilities triaged within established timeline b) 100% resolution rate of assigned vulnerabilities	100% Inspection
SS – 8 Provide a dedicated account team with customer support and success functions	1.3.9	a) 95% of customer support tickets acknowledged within 24 hours b) 90% resolution within five business days	Customer complaint

2.2 DELIVERABLES SUMMARY

All deliverables will be inspected for content completeness, accuracy, and conformance to requirements by the COR. Inspection may include validation of information or software by automated tools, testing, demonstrations, or inspections of the deliverables, as specified in the contract. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.
The Government requires a period NTE 15 business days after receipt of final deliverable items for inspection and acceptance or rejection.

For software or documents that may be proprietary, COTS or custom, RS/LD rights apply to proprietary COTS software or documents and UR rights apply to custom software or documents. The Government asserts UR rights to open-source COTS software.

The Government does not assert any rights to management software tools if the contractor does not plan to charge the Government directly for that tool and does not propose that the Government will own or use that tool.

Deliverables are due the next Government workday if the due date falls on a holiday or weekend. A “workday” is considered any day in a normal business day.

The contractor shall deliver the deliverables listed in the following table on the dates specified:

Table 2: Milestone/Deliverable Summary

DEL. #	MILESTONE/ DELIVERABLE	PWS REFE	DATE OF COMPLETION/ DELIVERY
1	Two enterprise management system licenses/subscriptions for DC3's DoD VDP and DIB VDP	1.3	Within 10 business days of contract award
2	Vulnerability submission and management workflows	1.3.2	As required
3	Crowdsourced vulnerability – bug tag and annual mailings	1.3.3	As required
4	Kickoff Meeting	1.4.1	Within 10 business days of contract award
5	Kickoff Meeting Agenda	1.4.2	Three business days prior to kickoff meeting
6	Transition Plan	1.4.3	Submitted as part of proposal
7	Transition Out Plan	1.5.1	Draft within three months of PS/Final due 10 calendar days after receipt of Government comments
8	Problem Notification Report PNR	2.8	As required

2.3 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by electronic mail (email) and removable electronic media, as well as placing in the DC3 VDP designated repository. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

Text	MS Word
Spreadsheets	MS Excel
Briefings	MS PowerPoint
Drawings	MS Visio
Schedules	MS Excel (Preferred); MS Project

2.4 PLACE(S) OF DELIVERY

Unclassified copies of all deliverables shall be delivered to the COR, and/or CO. The name, address, and contact information of these individuals will be provided at award.

2.5 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the contract and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

The Government requires a period NTE 15 business days after receipt of final deliverable items for inspection and acceptance or rejection. Final acceptance will occur when all discrepancies,

errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables shall either be incorporated in the succeeding version of the deliverable, or the contractor shall explain to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the quality assurance requirements stated within this contract, the document may be rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the COR.

2.4 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 business days from Government receipt of the draft deliverable. Upon receipt of the Government comments, the contractor shall have ten business days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

2.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The CO or COR will provide written notification of acceptance or rejection (**Section 2**) of all final deliverables within 15 business days. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

2.6 MARKINGS

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this contract. The Government reserves the right to treat nonconforming markings in accordance with subparagraphs (e) and (f) of the Defense Federal Acquisition Regulation Supplement (DFARS) 252.227-7013 and 252.227-7014. The contractor shall also mark each deliverable with proper security markings in accordance with Controlled Access Program Coordination Office (CAPCO) Authorized Classification and Control Markings.

2.7 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies shall be corrected, by the contractor, within ten business days of the rejection notice. If the deficiencies cannot be corrected within ten business days, the contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within ten business days.

If the contractor does not provide products or services that conform to the requirements of this contract, the Government will document the issues associated with the non-conforming products or services.

2.8 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The contractor shall notify the COR via a Problem Notification Report (PNR) **(Section 2, Deliverable 8)** as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

3.0 GOVERNMENT-FURNISHED PROPERTY/EQUIPMENT (GFE/GFI)

3.1 GOVERNMENT FURNISHED EQUIPMENT (GFE).

The Government may provide equipment to the contractor for work required under this contract. The contractor shall use GFE only for performing work under this contract, and it shall be responsible for returning all GFE to the Government at the end of the performance period. The contractor shall not release GFE to outside parties without the prior and explicit consent of the CO.

In accordance with DAFI 23-111, the contractor shall establish and maintain a controlled environment for the accountability of property.

3.2 GOVERNMENT-FURNISHED INFORMATION (GFI)

The Government will provide all necessary information, data, and documents to the contractor for work required under this contract. The contractor shall use GFI, data, and documents only for performing work under this contract, and it shall be responsible for returning all GFI, data, and documents to the Government at the end of the performance period. The contractor shall not release GFI, data, and documents to outside parties without the prior and explicit consent of the CO.

4.0 GENERAL INFORMATION

4.1 PERIOD OF PERFORMANCE

The period of performance for this contract is anticipated to include a 12-month base period and one, six-month option periods.

Base Period:	February 1, 2026 through January 31, 2027
First Option Period:	February 1, 2027 through January 31, 2028
Second Option Period:	February 1, 2028 through January 31, 2029
Third Option Period:	February 1, 2029 through January 31, 2030
Forth Option Period:	February 1, 2030 through January 31, 2031

4.2 PLACE OF PERFORMANCE

Place(s) of Performance under this contract include contractor and Government site locations.

4.3 PERFORMANCE SCHEDULE

4.3.1 RECOGNIZED HOLIDAYS

DC3 is closed for observed holidays, local or national emergencies, occasional administrative reasons, or similar Government directed closings.

4.3.2 HOURS OF OPERATION

In general, the contractor shall operate during normal DC3 business hours, Monday through Friday, from 8:00 a.m. to 5:00 p.m. Eastern Time (ET).

4.3.4 INCLEMENT WEATHER

The Contractor shall follow guidance of the installation containing their place of performance to determine reporting schedules whether due to a base closure or inclement weather. The website for guidance regarding status of performance for work to be performed in the National Capital Region (NCR) is http://www.opm.gov/status/.

4.4 TRAVEL

Travel is not associated with this contract.

4.5 SECURITY REQUIREMENTS

The DD Form 254 is applicable to this requirement. The contractor shall have a final TS Facility Clearance (FCL) from the Defense Counterintelligence and Security Agency (DCSA) Facility Clearance Branch (FCB). Upon formal notification by the contracting officer, the contractor shall have readily available access to DCSA-certified work locations for performing classified work up to and including TS/SCI within 60 calendar days of notification. The contractor and all subcontractors must possess the required security clearance, based on job requirements, prior to performing functions on the contract. The contractor and all subcontractors must maintain the required security clearance throughout the life of the contract. The contractor shall use only U.S. citizens to perform work under the requirements of this TO unless a waiver is approved by the Government. The contractor shall provide security clearance information to the DC3 Security and Information Assurance Offices.

4.5.1 INFORMATION ASSURANCE

The contractor may have access to sensitive (to include privileged and classified) data, information, and materials of the U.S. Government. These printed and electronic documents are for internal use only and remain the sole property of the U.S. Government. Some of these materials are protected by the Privacy Act of 1974 (AMENDED) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

Work on this contract may require that personnel have access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S.C, Section 552A and applicable DC3 rules and regulations.

4.5.2 SECURITY CLEARANCES

The security clearance level of DC3 contractor personnel is determined by their role held with this contract. The classification levels required can vary depending upon necessary access to specific systems and material.

The Contractor shall establish and implement methods of ensuring that no building access instruments issued by the Government are lost, misplaced or used by unauthorized persons. Access codes shall not be shared with any person(s) outside the organization. The Contractor shall control access to all Government provided lock combinations to preclude unauthorized entry. The Contractor is not authorized to record lock combinations without written approval by the Government COR. Records with written combinations to authorized secure storage containers, secure storage rooms, or certified vaults, shall be marked and safeguarded at the highest classification level as the classified material maintained inside the approved containers.

In general, all necessary facility and employee security clearances shall be at the expense of the contractor. The contractor shall comply with all security requirements.

4.5.3 INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR)

The requirements of this contract require presenting, discussing, and engaging in technical discussions (defense services) involving ITAR-controlled technical data with the Government Defense Agencies. In order for the contractor (including subcontractors, consultants, and teaming partners) to engage in technical discussions (defense services) with a foreign person, it shall be ITAR-compliant with either a Technical Assistance Agreement (TAA) or an ITAR Exemption authorizing export privileges with the cooperative partners. ITAR compliance means being registered with the U.S. Department of State (DoS) and having the proper ITAR authorizations to conduct defense services. In order to submit a request for ITAR authorization, the U.S. applicant (including all subcontractors, consultants, and teaming partners) must be registered with the Directorate of Defense Trade Controls (DDTC) and DoS, and the registration shall be current (renewable each year). The current list of countries for which an ITAR license will be required will be provided at contract award. The contractor shall maintain and update, as needed, a list of the approved ITARS licenses needed to support Cyber Threat Emulation (CTE). The offeror shall have TAAs in place within 90 calendar days of contract start date.

4.5.4 CYBERSECURITY WORKFORCE MANAGEMENT PROGRAM

Designated contractor personnel performing IT or Information Assurance (IA) related functions in support of this contract may require applicable certifications in accordance with DoD Directive (DoDD) 8140.01.

4.6 ORGANZIATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

4.6.1 ORGANIZATIONAL CONFLICT OF INTEREST

If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI to the CO in accordance with FAR Subpart 9.4. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.

The contractor is required to complete and sign an OCI Statement. The contractor must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this contract, or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below.

If the contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.

In addition to the mitigation plan, the CO may require further information from the contractor. The CO will use all information submitted by the contractor, and any other relevant information, to determine whether an award to the contractor may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.

If any such conflict of interest is found to exist, the CO may determine that the conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the contractor may be found ineligible for award. Alternatively, the CO may determine that it is otherwise in the best interest of the U.S. to contract with the contractor and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded.

4.6.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) Form and ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the contract:

Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.

Are instructed in FAR Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel shall also be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this contract or obtained from the Government is only to be used in the performance of the contract. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

4.7 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 U.S.C. 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

4.8 CONTRACTOR IDENTIFICATION

Contractor personnel shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and by displaying distinguishing badges or other visible identification for meetings with Government personnel. Contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

4.9 CONTRACT CLOSEOUT

The Government will unilaterally close out the contract no later than six years after the end of the contract period of performance if the contractor does not provide final DCAA rates by that time.

4.10 PRESS/NEWS RELEASE

The contractor shall not make any press/news release pertaining to this procurement without prior Government approval and only in coordination with the CO.

4.11 QUALITY

Quality Assurance. The Government shall rely on the Contractors' existing quality assurance system as the method to ensure that the requirements of the contract and performance thresholds are met; however, the Government reserves the right to monitor and evaluate the quality of services provided and compliance with the contract terms and conditions at any time.

Quality Control Plan (QCP). The Contractor shall develop and maintain an effective quality control program to ensure services are performed IAW this PWS, applicable laws and regulations, and best commercial practices. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services with special emphasis placed on those services listed in this PWS. The Contractor's quality control program is the means by which it assures itself that the work complies with the requirement of the contract

4.12 EMERGENCY OPERATIONS/MISSION ESSENTIAL PERSONNEL

Continuation of Essential Contractor Services During Crisis. All services in this PWS HAVE NOT been defined or designated as essential services for performance during crisis IAW DFARs 252.237-7023, "Continuation of Essential Contractor Services."

4.13 SYSTEM FOR AWARD MANAGEMENT (formerly CMRA)

The Contractor shall report ALL labor hours (including subcontractor labor hours) required for performance of services provided under this contract via the System for Award Management (SAM) data collection site. The Contractor is required to completely fill in all required data fields at http://www.SAM.gov. Reporting inputs shall be for the labor executed during the period of performance for each Government fiscal year (FY), which runs 1 October through 30 September. The UIC for AFDW is FF16M0. While inputs may be reported anytime during the FY, all data shall be reported not later than 31 October of each calendar year. The Contractor may direct questions to the System for Award Management help desk.

Subcontractor Input in SAM. Prime Contractors are responsible to ensure all subcontractor data is reported. Subcontractors will not be able to enter any data into SAM, but will enter their information into a Bulk Loader spreadsheet available from the SAM helpdesk. Subcontractor shall fill in columns A-C then return it to the SAM helpdesk after it's completed and a technician team will enter the information into SAM

4.14 MISCELLANEOUS PARAGRAPHS

4.14.1 Freedom of Information Act (FOIA). All official Government records affected by this contract are subject to the provisions of the FOIA (5 U.S.C. 552/DoD 5400.7-R/AF Supplement). Any request received by the Contractor for access/release of information from these records to the public (including Government/Contractor employees acting as private citizens), whether oral or in writing, shall be immediately brought to the attention of the CO for forwarding to the FOIA Manager to ensure proper processing and compliance with the Act.

4.14.2 Controlled Unclassified Information (CUI). All DoD CUI must be controlled until authorized for public release in accordance with DoD Instructions (DoDIs) 5230.09, 5230.29, and 5400.04, or DoD Manual (DoDM) 5400.07. These regulations set policy and procedures for the disclosure of records to the public and for marking, handling, transmitting, and safeguarding of CUI material.

4.14.3 Privacy Act. Work on this contract may require that personnel have access to information protected by the Privacy Act. Contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations when handling such information.

4.14.4 Records. All records created and received by the Contractor in the performance of this contract shall be maintained in a single, CAC enabled, repository, accessible to the Government. Records shall remain the property of the Government.

4.14.5 Safety Concerns. The Contractor is solely responsible for compliance with OSHA standards for the protection of their employees. The Government is not responsible for ensuring that Contractors comply with “personal” safety requirements that do not present the potential to damage Government resources.

4.14.6 Project Policy. The Contractor shall comply with all industry standards. All work shall be done in accordance with all federal, local, and state laws and regulations.

4.14.7 Inherently Governmental Functions. The Contractor shall not perform inherently Governmental functions as defined in the Federal Acquisition Regulation (FAR) Subpart 7.5 in relation to this PWS.

4.14.8 Ethics. The Contractor shall not employ any person who is an employee of the US Government if employing that person would create a conflict of interest. Additionally, the Contractor shall not employ any person who is an employee of the Department of the Air Force, either military or civilian, unless such person seeks and receives approval according to DoDD 5500-7, Joint Ethics Regulation.

4.14.10 Non-Personal Services. The Government shall not supervise or task Contractor employees in any manner that generates actions of the nature of personal services, or that creates the perception of personal services. It is the responsibility of the Contractor to manage its employees directly and to guard against any actions that are of the nature of personal services, or give the perception of personal services to the Government or to Government personnel. If the Contractor feels that any actions constitute, or are perceived to constitute personal services, it is the Contractor's responsibility to notify the CO immediately. Non-personal Contractor services shall not be used to perform work of a policy/decision making or management nature.