

## **SECTION C – DESCRIPTION/SPECS/WORK STATEMENT**

### **SPECIFICATIONS/STATEMENT OF WORK/PERFORMANCE WORK STATEMENT**

Work under this performance-based task order will be performed in accordance with the following description/ specifications/ statement of work (SOW) which herein will be referred to as Performance Work Statement (PWS):

### **SHORT TITLE: CYBERSECURITY ASSESSMENT AND AUTHORIZATION SUPPORT II**

#### **1.0 PURPOSE**

##### **1.1 SCOPE**

Naval Information Warfare Center (NIWC) Atlantic is delivering Defensive Cyber Operations (DCO) for a range of Department of Defense (DoD) and federal networks, aiming to align with an organization that provides DCO services. This contract will provide Cybersecurity Assessment and Authorization support to sites located throughout the Continental United States (CONUS) and Outside the Continental United States (OCONUS), ranging in size from 1,500 to over 60,000 server and workstations across over 400 Programs of Record Systems of varying size, architecture and operating systems.

The scope of this task order encompasses a range of cybersecurity support services for the Department of Defense (DoD), Defense Health Agency (DHA) Joint, Coalition, Non-DoD, and other Federal Government agencies. The contractor shall provide expertise in testing, validating, and supporting cybersecurity-enabled systems, including specific platforms like ACAS, HBSS, and network devices. A significant portion of the work focuses on Assessment and Authorization (A&A) activities, aligning with the Risk Management Framework (RMF) and supporting compliance with DoD cybersecurity directives. This includes developing and reviewing security assessment plans, conducting security control assessments, and supporting Independent Verification and Validation (IV&V) efforts. The scope also includes enhancing and maintaining DHA's cybersecurity toolsets, focusing on streamlining testing events, automating processes, and improving the accuracy of assessments. The contractor will provide program office RMF support, developing RMF documentation, and conducting self-assessments. Furthermore, the contractor will support privacy and Health Insurance Portability and Accountability Act (HIPAA) compliance efforts, including performing risk assessments, maintaining documentation, and monitoring compliance. Finally, technical support includes developing cybersecurity documentation, reports, and training materials.

NOTE: Website and e-mail addresses referenced within the PWS and Contract Data Requirements List (CDRL) forms are subject to change. For any website and e-mail address not working during time of performance, the contractor shall contact the Contracting Officer's Representative (COR) or Contracting Officer for latest website and e-mail address. An incorrect website or e-mail address does not alleviate a contractor from required reporting or access requirements.

#### **2.0 PLACE(S) OF PERFORMANCE**

##### **2.1 GOVERNMENT FACILITIES**

Government facilities (i.e., office space or lab space) are provided to those contractor personnel that would otherwise adversely affect the work performance if they were not available on Government site. Labor categories with supplied Government facilities shall be located at:

- NIWC Atlantic, Charleston, SC
- NIWC Atlantic, Stuttgart, Germany
- NIWC Pacific, Honolulu, Hawaii

#### 2.1.1 Access to Government facilities

NIWC Atlantic and other Government installations have restricted access. Contractors are limited to access during certain days and times as specified in the workweek requirements of this PWS. If access to the assigned Government facility is restricted due to safety/security exercise, an Executive Order, or an administrative leave determination applying to the local activity (e.g., inclement weather), the contractor, in agreement with the COR, shall make alternative work arrangements. The contractor shall adjust work schedule, work at an alternate location, or if alternate work arrangements cannot be accommodated, the contractor shall notify the COR of the inability to access the assigned facility prior to charging their time to the task order as direct cost provided such charges are consistent with the contractor's accounting practices.

#### 2.1.2 Training Requirements and Exercise Support

Contractor personnel working full-time or partially at a Government facility shall complete all applicable training requirements as specified under Mandatory Training, PWS Para 8.0. Contractor personnel may also be required to participate in safety, security (e.g., Anti-Terrorism Force Protection (AT/FP)), and operational training exercises (possibly two per year). Applicable contractor personnel shall support and participate in the training exercise which may include role-playing and reacting to exercise injects based on the situation or exercise objectives.

#### 2.1.3 Emergency Management at Government Installations

During emergency situations including health (e.g., COVID-19 pandemic) and weather-related circumstances, contractor personnel with scheduled access to a Government installation shall coordinate with the COR prior to reporting to their Government worksite. Access will be in accordance with the latest Government installation requirements and restrictions. The contractor shall identify with the COR if certain personnel are designated mission essential and determine the work expectations during the emergency period of performance. Depending on the type of support, working from an alternative worksite may or may not be allowed.

#### 2.1.4 German Status of Forces Agreement (SOFA)

GERMANY ACCREDITATION- SOFA and the **BACO-90 Process** are hereby incorporated.

1. The DoD Contractor Personnel Office (DOCPER) implements the Agreements of 27 March 1998, and the Agreements of 29 June 2001, signed by the U.S. Embassy and German Foreign Ministry, establishing bilateral implementation of Articles 72 and 73 of the Supplementary Agreement (SA) to the NATO SOFA. These two Articles govern the use in Germany of DoD contractor employees as Technical Experts (TE), Troop Care (TC) providers, and Analytical Support (AS) contractor personnel. Army in Europe and Africa (AE) Regulation (Reg) 715-9 contains most information needed regarding status accreditation under Articles 72 and 73.

2. Temporary Duty (TDY) status can be obtained through a process referred to as the **BACO-90 Process**. Refer to DOCPER for the procedures and submission requirements associated with this type application.

3. Under both procedures above, prior approval is required *before* contractor employees may begin work in Germany under the contract.

### 2.2 CONTRACTOR FACILITIES

A significant portion of work issued under this task order requires close liaison with the Government. The contractor shall be prepared to establish a local facility within a fifteen (15)-mile radius of NIWC Atlantic. This fifteen (15)-mile radius is needed for frequent collaboration efforts between the Government and Contractor personnel and the requirement for personnel to travel from NIWC at JB

Charleston to the contractor site multiple times a week for meetings and collaboration within the NIWC lab space for cybersecurity analysis, testing, and evaluation. The contractor shall be capable of quickly interfacing with the labs located at NIWC Atlantic. The contractor's facility is not necessarily for the exclusive use of this task order and can be utilized on a shared basis. The contractor shall meet all facility requirements within 30 days after task order award. The contractor's facility shall include physical security to protect Government property as identified in PWS Para10.0. The contractor shall ensure facility configuration includes space for offices, conference rooms, lab work, and a staging area for materials and equipment.

## 2.3 ALTERNATE WORK LOCATIONS

The ability to provide support from an alternate location (includes working from an employee's residence or other non-Government facility) is dependent on the type of support required, the contractor employee's ability and trustworthiness, and the company's employment policy. Allowing work to be performed at an alternate location is not an option for all positions and personnel. The ultimate decision to allow work performed at an alternate work location will be determined by the COR. If alternate work locations are allowed, the company shall have defined criteria addressing the minimum requirement to have continuous, secure internet connectivity. Each applicable contractor employee shall have an established signed telework agreement between the company and employee. For each contractor employee proposed to work at an alternate location, the contractor shall submit a written request and justification to the COR with a copy of the applicable employee's signed telework agreement which becomes part of the COR files. If the requirements for teleworking and/or alternate work locations are not outlined/specified in the employee agreement documentation, the contractor shall include a copy of those requirements with the signed employee agreement. Working at an alternative location shall not adversely affect the response time required in support of the task order. The Government reserves the right to discontinue the ability to work from an alternate location at any time without cause. The inability of a contractor to respond to the requirements of the task order due to telework conditions will be negatively reflected in the Contractor Performance Assessment Reporting System (CPARS).

The following alternate work location support is projected but are subject to change with COR concurrence:

<b>PWS Task Paragraph</b>	<b>Alternate work location Allowed</b>
3.3.2, 3.4.2, 3.6.2	No
All Other Tasking	Yes

## 2.4 SPECIFIC LOCATIONS

This order requires a Top Secret facility clearance with access to Sensitive Compartmented Information (SCI). The contractor shall provide support and resources that meet all security requirements for special access at the following locations:

a. see Attachment #2 (*the location list will be disclosed to only the awardee at time of award*)

## 3.0 PERFORMANCE REQUIREMENTS

The following paragraphs list non-personal services tasks that will be required throughout this task order. The contractor shall provide necessary resources with knowledge and experience as cited in the personnel qualification requirement to support the listed tasks. The contractor shall perform requirements in accordance with Federal Acquisition Regulation (FAR) and/or Defense Federal Acquisition Regulation Supplement (DFARS) that do not include performance of inherently

Government functions. The contractor shall complete all required tasks while controlling and tracking performance and goals in terms of costs, schedules, and resources.

### 3.1 RELEVANT EXPERIENCE

#### 3.1.1 Systems and Equipment

The contractor shall provide functional and technical expertise testing, validating, and supporting a wide range of DoD Cybersecurity enabled systems. Systems will range from client-server applications employing interactive and batch processes to customized web-based solutions operating in a distributed or standalone environment. Such systems include, but are not limited to:

- Assured Compliance Assessment Solution (ACAS)
- Host Based Security System (HBSS)
- Microsoft Endpoint Configuration Manager (MECM)
- CrowdStrike
- IP-based network enabled medical devices Enhanced Mitigation Experience Toolkit (EMET) Group Policy Objects (GPOs)
- Security Information Event Managers (SIEM)
- Intrusion detection and prevention systems (IDS and IPS)
- Network devices; including routers, firewalls, switches, and web proxies

#### 3.1.2 Programs and Initiatives

The contractor shall have expertise supporting and complying with DHA and/or DoD enterprise Cybersecurity initiatives. Such programs and initiatives include at a minimum:

- Risk Management Framework (RMF)
- Continuous Monitoring and Risk Scoring (CMRS)
- Consolidated System Tracking and Reporting (CSTAR)
- Enterprise Mission Assurance Support Service (eMASS)

### 3.2 PROGRAM MANAGEMENT

The contractor shall assist the Government project manager providing support at the sponsor level.

#### 3.2.1 Program Support

The contractor shall work closely with the Government project manager supporting the needs of the program at the sponsor level. Requirements include coordinating meetings, preparing budget drills, developing agenda items and status briefings, attending high-level meetings, generating minutes, and tracking action items. Additionally, the contractor shall utilize analysis of actual outcomes or their expert opinion to recommend policies, doctrine, tactics, and procedures at the Federal, State, and Local level. Program support will require significant coordination and interface with various DoD and non-DoD activities located in and out of the CONUS.

#### 3.2.2 Program Support Documentation

The contractor shall develop and draft various Program Management (PM) reports (CDRL A001). The following documents are typical PM Deliverables that the contractor shall have knowledge writing:

- Agendas

- Briefs
- Cost Estimation
- DHA / Service RMF Program Cybersecurity budgeting Meeting Agenda and Minutes
- Plans of Action and Milestones (POA&M) Work Breakdown Structure (WBS) Alignment
- Accounting Classification Reference Number (ACRN) Alignment (e.g. Navy ACRN AA, NCR ACRN AB)
- Labor Hours Information Fully Burdened Rates
- Costs for Other Direct Costs (ODCs) (Travel, Materials, etc.) Funds Forecast (i.e. Spend Plans)
- Various Program Acquisition related documents: Mission Needs Statement (MNS), Capability Production Documentation (CPD), Operational Requirements Document (ORD), etc.
- Weekly reports on RMF status for system/enclave(s) (CDRL A002)
- Travel and leave tracker (CDRL A003)
- Cost estimate for System/Enclave (CDRL A004)
- Available budget and expensed funding at system/enclave level (CDRL A005)

### 3.3 SECURITY CONTROLS ASSESSOR/REPRESENTATIVE (SCA/(R)) SUPPORT (MISSION ESSENTIAL CONTRACTOR SERVICES)

#### 3.3.1 SCA/(R) Support

For tasking requiring Secret clearance as determined by the Government, the contractor shall provide the following support:

3.3.1.1 The contractor shall provide subject matter expertise to develop plans (CDRL A006) and review plans to assess the security controls.

3.3.1.2 The contractor shall assess the security controls in accordance with the assessment procedures defined in the security assessment plan.

3.3.1.3 The contractor shall prepare the security assessment report (CDRL A006) documenting the issues, findings, and recommendations from the security control assessment (SCA).

3.3.1.4 The contractor shall conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s) as appropriate.

3.3.1.5 The contractor shall assess a selected subset of the technical, management, and operational security controls employed within and inherited by information systems in accordance with the organization defined monitoring strategy.

#### 3.3.2 SCA/(R) Support

For tasking requiring TS-SCI clearance as determined by the Government, the contractor shall provide the following support:

3.3.2.1 The contractor shall provide subject matter expertise to develop plans (CDRL A006) and review plans to assess the security controls.

3.3.2.2 The contractor shall assess the security controls in accordance with the assessment procedures defined in the security assessment plan.

3.3.2.3 The contractor shall prepare the security assessment report (CDRL A006) documenting the issues, findings, and recommendations from the security control assessment (SCA).

3.3.2.4 The contractor shall conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s) as appropriate.

3.3.2.5 The contractor shall assess a selected subset of the technical, management, and operational security controls employed within and inherited by information systems in accordance with the organization defined monitoring strategy.

### 3.4 ASSESMENT AND AUTHORIZATION (A&A)

#### 3.4.1 A&A Support

For tasking requiring Secret clearance as determined by the Government, the contractor shall provide the following support:

3.4.1.1 The contractor shall support compliance with DoD Cybersecurity RMF Directives and Processes by:

- Providing assistance to system owner, enclave, or site personnel to complete required RMF documentation;
- Addressing Independent Validation and Verification (IV&V) results and assisting enclave personnel in preparing all aspects of an Enterprise Mission Assurance Support Service (eMASS) authorization package for review by the Validator, SCA(R), or the Authorizing Official (AO);
- Reviewing Security Design documentation to ensure comprehensive security requirements and compliance with DoD and Federal requirements and guidelines;
- Reviewing and providing input on physical, application, and networking security policies, procedures, and practices;
- Updating any A&A Standard Operating Procedures (SOP) so that it aligns to program policies;
- Providing documentation support in the form of assisting with the writing and production of SOPs and Operational Manuals, and reviewing Government established and created Policies and Procedures;
- Supporting the implementation of Federal IT Security regulations, directives and guidance (Federal Information Security Management Act - FISMA, Federal Information Processing Standard FIPS, National Institute of Standards and Technology - NIST series);
- Documenting the cybersecurity test plan and procedures (CDRL A006) to appropriately relate the testing standard identified by the AO and SCA(R) activities.

3.4.1.2 The contractor shall support A&A Program Efforts with stakeholders by:

- Reviewing updates of the RMF documentation from the system owner and tracking status of changes;
- Assisting in the development of the path to complete authorization;
- Assembling the RMF Package (CDRL A006), (RMF Scorecard, POA&M, assessment documentation, and RMF System Implementation Plans (SIPs) and delivering it to the SCA(R) in a trusted manner consistent with DHA and/or Program requirements;

- Providing A&A support in the areas of network topologies, file/application servers, encryption technologies, and network operating hardware and software;
- Assessing the eMASS package to include the completeness of the vulnerability POA&M;
- Tracking assigned system from initiation to retirement while staying informed of IV&V milestones and RMF POA&M deadlines;
- Addressing authorization questions from the Program Management Office (PMO);
- Maintaining authorization schedules, for systems and working with the PMO to ensure the correct A&A process is being followed;
- Adhering to all authorization guidance received from the SCA(R) and performing actions necessary to complete assessment;
- Participating in all test execution and planning activities, including meetings and working groups;
- Participating in RMF Team Meetings and System review related meetings and providing technical and non-technical guidance;
- Identifying and elevating the need for any additional cybersecurity test events needed to support authorization (includes scheduling of annual reviews)

3.4.1.3 The contractor shall support the Cybersecurity Validation Readiness review efforts for both sites/enclaves and programs of records by:

- Evaluating the self-assessment results and evidence during Readiness Review to determine if the security is sufficiently mature to execute an assessment test event;
- Determining the IV&V test level of effort for each planned system or enclave;
- Participating in all test execution and planning activities, including meetings and working groups;
- Reviewing the RMF documentation prior to IV&V to determine security readiness of system, site, or enclave

3.4.1.4 The contractor shall support all of the necessary RMF Independent Verification and Validation events assigned by:

- Supporting the IV&V testing of each system, site, or enclave under the SCA(R) and AO purview;
- Participating in all test execution and planning activities (CDRL A006), including meetings and working groups and provide all minutes and meeting notes (CDRL A001) IAW RMF process documents;
- Reviewing all RMF documentation to ensure the information is current, accurate, and applicable to the article of test;
- Supporting standardization, by ensuring that all cybersecurity test procedures are up to date with all current applicable requirements and that those methods of testing are widely visible and available to apply to all necessary systems across its enterprise;

- Producing all necessary RMF security controls test procedures (for inclusion in the Security Assessment Plan (CDRL A006)) that describe how to perform validation actions as outlined in the applicable Security Technical Implementation Guide (STIG) checklists;
- Analyzing previous cybersecurity testing artifacts to ensure proper tailoring of cybersecurity tests is considered and accounted for;
- Developing the Security Assessment Plan (SAP), providing to the system owner, documentation team, and A&A team (CDRL A006);
- Overseeing the execution of testing to identify all vulnerabilities, and documenting all residual risks by conducting thorough risk assessments;
- Providing the cybersecurity risk analysis and mitigation determination results for use in the test report;
- Developing and/or utilizing automated tools, for the creation of necessary test evidence, risk assessment, and authorization artifacts for each system;
- Performing wireless discovery using DoD approved software;
- Performing all testing with tools (see: 3.5) capable of managing the test procedures and results;
- Providing appropriately qualified validator and IV&V representatives to review all RMF documentation prior to IV&V;
- Scheduling the IV&V test events and assigning IV&V team members to meet the requirements of the Security Assessment Plan (CDRL A006);
- Providing all necessary status reports to the Government PM to document the progress/results of cybersecurity testing in accordance with requirements established in the IV&V level of effort determination. (CDRL A006)
- Coordinating the test planning with Subject Matter Experts (SMEs) identified from cybersecurity Validation Team with the SCA(R)

3.4.1.5 The contractor shall provide oversight and support of the POA&M and RMF Scorecard creation by:

- Overseeing the completion of the RMF Scorecard within eMASS;
- Providing any Government approved mitigation and remediation in support of the RMF process both remotely and on-site;
- Providing POA&M resolution recommendations to reduce residual risk in accordance with applicable DoD and Federal technical and operational requirements and guidelines (CDRL A006);
- Providing assistance to sites to update outstanding actions contained in the POA&M and assisting with the request of extensions for expiring ATOs or POA&M items;

3.4.1.6 The contractor shall provide formal RMF validation services of all submitted RMF packages within the eMASS instance by:

- Maintaining any qualified validator status, in accordance with applicable agency requirements;



- Reviewing all packages for accuracy and completeness before being delivered to SCA(R) and producing a risk assessment artifacts package completeness report. (CDRL A006);
- Working directly with the SCA(R) as a qualified agent to ensure validation activities are compliant with the cybersecurity test strategy;
- Conducting in-depth analysis of IV&V, A&A, and functional/operational test results for accuracy, compliance, and adherence to DoD and Federal cybersecurity technical and operational security requirements;
- Working with the system owner or program manager to develop specific site or system mitigation to achieve an overall reduction in residual risk;
- Coordinating with the SCA(R) and providing consult for the issuance of a proper authorization recommendation that complies with all applicable DoD and Federal guidance.

3.4.1.7 The contractor shall provide support in performing proper risk assessments in accordance with all applicable DHA and/or DoD and Federal requirements by:

- Conducting in-depth analysis of IV&V, A&A, and functional/operational test results for accuracy, compliance, and adherence to DoD and Federal cybersecurity technical and operational security requirements; (CDRL A006)
- Documenting residual risks by conducting a thorough review of all the vulnerabilities, architecture and defense in depth and providing the cybersecurity risk analysis and mitigation determination results (CDRL A006) for any required test or risk reports;
- Assisting the SCA(R) and/or Validator with producing the risk assessment artifacts describing residual risks identified during testing or analysis (CDRL A006).

#### 3.4.2 A&A Support

For tasking requiring TS-SCI clearance as determined by the Government, the contractor shall provide the following support:

3.4.2.1 The contractor shall support compliance with DoD Cybersecurity RMF Directives and Processes by:

- Providing assistance to system owner, enclave, or site personnel to complete required RMF documentation;
- Addressing Independent Validation and Verification (IV&V) results and assisting enclave personnel in preparing all aspects of an Enterprise Mission Assurance Support Service (eMASS) authorization package for review by the Validator, (SCA(R), or the Authorizing Official (AO));
- Reviewing Security Design documentation to ensure comprehensive security requirements and compliance with DoD and Federal requirements and guidelines;
- Reviewing and providing input on physical, application, and networking security policies, procedures, and practices;
- Updating any A&A Standard Operating Procedures (SOP) so that it aligns to program policies;

- Providing documentation support in the form of assisting with the writing and production of SOPs and Operational Manuals, and reviewing Government established and created Policies and Procedures;
- Supporting the implementation of Federal IT Security regulations, directives and guidance (Federal Information Security Management Act - FISMA, Federal Information Processing Standard FIPS, National Institute of Standards and Technology - NIST series);
- Documenting the cybersecurity test plan and procedures (CDRL A006) to appropriately relate the testing standard identified by the AO and SCA(R) activities.

3.4.2.2 The contractor shall support A&A Program Efforts with stakeholders by:

- Reviewing updates of the RMF documentation from the system owner and tracking status of changes;
- Assisting in the development of the path to complete authorization;
- Assembling the RMF Package (CDRL A006), (RMF Scorecard, POA&M, assessment documentation, and RMF System Implementation Plans (SIPs) and delivering it to the SCA(R) in a trusted manner consistent with DHA and/or Program requirements;
- Providing A&A support in the areas of network topologies, file/application servers, encryption technologies, and network operating hardware and software;
- Assessing the eMASS package to include the completeness of the vulnerability POA&M;
- Tracking assigned system from initiation to retirement while staying informed of IV&V milestones and RMF POA&M deadlines;
- Addressing authorization questions from the Program Management Office (PMO);
- Maintaining authorization schedules for systems and working with the PMO to ensure the correct A&A process is being followed;
- Adhering to all authorization guidance received from the SCA(R) and performing actions necessary to complete assessment;
- Participating in all test execution and planning activities, including meetings and working groups;
- Participating in RMF Team Meetings and System review related meetings and providing technical and non-technical guidance;
- Identifying and elevating the need for any additional cybersecurity test events needed to support authorization (includes scheduling of annual reviews)

3.4.2.3 The contractor shall support the Cybersecurity Validation Readiness review efforts for both sites/enclaves and programs of records by:

- Evaluating the self-assessment results and evidence during Readiness Review to determine if the security is sufficiently mature to execute an assessment test event;
- Determining the IV&V test level of effort for each planned system or enclave;

- Participating in all test execution and planning activities, including meetings and working groups;
- Reviewing the RMF documentation prior to IV&V to determine security readiness of system, site, or enclave

3.4.2.4 The contractor shall support all of the necessary RMF Independent Verification and Validation events assigned by:

- Supporting the IV&V testing of each system, site, or enclave under the SCA(R) and AO purview;
- Participating in all test execution and planning activities (CDRL A006), including meetings and working groups and provide all minutes and meeting notes (CDRL A001) IAW RMF process documents;
- Reviewing all RMF documentation to ensure the information is current, accurate, and applicable to the article of test;
- Supporting standardization, by ensuring that all cybersecurity test procedures are up to date with all current applicable requirements and that those methods of testing are widely visible and available to apply to all necessary systems across its enterprise;
- Producing all necessary RMF security controls test procedures (for inclusion in the Security Assessment Plan (CDRL A006)) that describe how to perform validation actions as outlined in the applicable Security Technical Implementation Guide (STIG) checklists;
- Analyzing previous cybersecurity testing artifacts to ensure proper tailoring of cybersecurity tests is considered and accounted for;
- Developing the Security Assessment Plan (SAP), providing to the system owner, documentation team, and A&A team (CDRL A006)
- Overseeing the execution of testing to identify all vulnerabilities, and documenting all residual risks by conducting thorough risk assessments;
- Providing the cybersecurity risk analysis and mitigation determination results for use in the test report;
- Developing and/or utilizing automated tools, for the creation of necessary test evidence, risk assessment, and authorization artifacts for each system;
- Performing wireless discovery using DoD approved software;
- Performing all testing with tools (see 3.5) capable of managing the test procedures and results;
- Providing appropriately qualified validator and IV&V representatives to review all RMF documentation prior to IV&V;
- Scheduling the IV&V test events and assigning IV&V team members to meet the requirements of the Security Assessment Plan (CDRL A006);
- Providing all necessary status report to the Government PM to document the progress/results of cybersecurity testing in accordance with requirements established in the IV&V level of effort determination. (CDRL A006)

- Coordinating the test planning with Subject Matter Experts (SMEs) identified from cybersecurity Validation Team with the SCA(R)

3.4.2.5 The contractor shall provide oversight and support of the POA&M and RMF Scorecard creation by:

- Overseeing the completion of the RMF Scorecard within eMASS;
- Providing any Government approved mitigation and remediation in support of the RMF process both remotely and on-site;
- Providing POA&M resolution recommendations to reduce residual risk in accordance with applicable DoD and Federal technical and operational requirements and guidelines (CDRL A006);
- Providing assistance to sites to update outstanding actions contained in the POA&M and assisting with the request of extensions for expiring ATOs or POA&M items;

3.4.2.6 The contractor shall provide formal RMF validation services of all submitted RMF packages within the eMASS instance by:

- Maintaining any qualified validator status, in accordance with applicable agency requirements;
- Reviewing all packages for accuracy and completeness before being delivered to SCA(R) and producing a risk assessment artifacts package completeness report. (CDRL A006);
- Working directly with the SCA(R) as a qualified agent to ensure validation activities are compliant with the cybersecurity test strategy;
- Conducting in-depth analysis of IV&V, A&A, and functional/operational test results for accuracy, compliance, and adherence to DoD and Federal cybersecurity technical and operational security requirements;
- Working with the system owner or program manager to develop specific site or system mitigation to achieve an overall reduction in residual risk;
- Coordinating with the SCA(R) and providing consult for the issuance of a proper authorization recommendation that complies with all applicable DoD and Federal guidance.

3.4.2.7 The contractor shall provide support in performing proper risk assessments in accordance with all applicable DHA and/or DoD and Federal requirements by:

- Conducting in-depth analysis of IV&V, A&A, and functional/operational test results for accuracy, compliance, and adherence to DoD and Federal cybersecurity technical and operational security requirements (CDRL A006);
- Documenting residual risks by conducting a thorough review of all the vulnerabilities, architecture and defense in depth and providing the cybersecurity risk analysis and mitigation determination results (CDRL A006) for any required test or risk reports;
- Assisting the SCA(R) and/or Validator with producing the risk assessment artifacts describing residual risks identified during testing or analysis (CDRL A006).

### 3.5 CYBERSECURITY TOOL/TOOLSET ENHANCEMENT AND MAINTENANCE

3.5.1 The contractor shall provide appropriate program workflow experts and web developers to support the enhancement and maintenance of SharePoint enabled web-based solution for a community-wide data collection and management system whose primary function is to:

- Expedite and streamline the process of tracking and reporting systems to program leadership, A&A Users, System Owners and PMOs;
- Provide Rollup Dashboard functionality to display system and authorization metrics from each underlying service;
- Provide Service level dashboards with filtered reports for each service;
- Increase visibility to the PMOs and System owners for their systems;
- Support managing the A&A processes across services;
- Track process steps (RMF and other applicable processes);
- Provide centralized portal for stakeholders to submit system/enclave associated issues and notes.

3.5.2 The contractor shall provide appropriately skilled application programming experts to support the enhancement and maintenance of the program's cybersecurity tool/toolset (including DISA provided tools) used in the assessment and authorization process. This tool/tools currently/should maintain the ability to streamline testing events within the programs and enclaves by supporting the following non-exclusive requirements, while maintaining 100% accuracy and transparency:

- Analyze raw ACAS results and automatically produce a report
- Automation of inventories and providing a detailed, error-free report;
- Automation, identification and assignment of IV&V STIGs – identifies what's required and auto assigns STIGs to relevant host, creates a test plan, applies sampling guidance and creates fully random sample groups;
- Creates detailed vulnerability report;
- Lists all open ports on each host, ID's firewall/IDS interference, maintains plugin version control, and identifies targeted IP ranges;
- Automate the assessment and consolidation of security scans of systems;
- Improve accuracy of assessment with a goal of 100% accuracy;
- Be easily executed and highly collaborative;
- Reduce security overhead lowering IT lifecycle costs

3.5.3 The contractor shall provide tool/tools to maintain the ability to streamline testing events within the programs and enclaves by supporting the following non-exclusive requirements, while maintaining 100% accuracy and transparency:

- Ability to apply selected security controls, overlays, and Control Correlation Identifier (CCI's) to later technical STIG selection to de-conflict N/A assessment procedures;

- Provides extensive search capabilities to research specific CCI or STIGs, general analyst inquiries, applicability research, etc;
- Ability to provide for the bulk exchange of asset, checklist, and assessment information (evidence, comments, status) between SCA, PMO, and other relevant parties (vendors or commercial contractors);
- Ability to create a Security Assessment Plan (SAP) or test matrix from imported and manually generated data;
- Support the manual manipulation of assets and scan results to facilitate SAP build (ex: assign checklists to assets, de-conflict CCIs and N/A cybersecurity Controls, etc);
- Ability to produce a level-of-effort estimate for a testing event, including number of personnel, length of test event and cost associated with test event. (CDRL A001);
- Support intelligent automatic assignment of STIGs or security checklists using assigned meta data and Common Platform Enumeration (CPE) information;
- Support creation of default evidence, comments, and statuses for particular CCIs and rules to facilitate a speedy assessment;
- Support integration with other automated tools and data formats to expedite accurate assessments by importing common DoD and industry standards, mapping and de-conflicting rules between automated scans and supporting future integration of changing standards (and backwards compatibility);
- Export raw evidence data in industry formats (ex: MITRE Extensible Configuration Checklist Description Format (XCCDF) or DoD CKL) and eMASS ready and customizable POAMs

### 3.6 PROGRAM OFFICE RMF SUPPORT (MISSION ESSENTIAL CONTRACTOR SERVICES)

#### 3.6.1 Program Office RMF Support

For tasking requiring Secret clearance as determined by the Government, the contractor shall provide the following support:

##### 3.6.1.1 The contractor shall provide RMF Documentation Support:

- Develop all RMF documentation in accordance with DoD/DHA policies and procedures to ensure that authorization packages are complete and system compliance accurately documented for the Authorizing Official (AO) (CDRL A006);
- Maintain Plan of Action and Milestones documentation;
- Work with the Program Management Office (PMO) to ensure that the correct RMF Process is being followed and participate in any required team meetings;
- Address authorization documentation questions from the PMO;
- Develop RMF documentation to ensure the information is current, accurate, and applicable to the article of test; (CDRL A006)

- Develop Cybersecurity self-assessment results and evidence during any Cybersecurity validation readiness reviews to determine if the system security is sufficiently mature to execute the Cybersecurity test event;
- Utilize Enterprise Mission Assurance Support Services (eMASS) and systems such as Continuous Monitoring and Risk Scoring (CMRS) for the documentation of test evidence and risk assessment for each system;
- Develop associated Cybersecurity artifacts to include, but not limited to, the System Security Plan, System Design and Architecture, Contingency Plan/Continuity of Operations Plan (COOP) Plan, Incident response Plan, Audit Design, Change Control Board, Identification and Authentication, Physical and Environmental, and Remote artifacts; (CDRL A006)
- Provide all necessary status report to the Government PM documenting the progress/results of Program Office RMF Support (CDRL A006)

#### 3.6.1.2 The contractor shall provide Self-Assessment Support:

- Work with Independent Verification & Validation (IV&V) Lead to develop test plans and participate in system related team meetings; (CDRL A006)
- Prepare for on-site self-assessments;
- Execute tests in accordance with test plans;
- Prepare test events status reports and out-briefs; (CDRL A006)
- Populate databases such as eMASS and CMRS with test results and provide input into test event reporting;
- Assemble Cybersecurity package [e.g. Scorecard, Plans of Action & Milestones (POA&M), Certification Documentation, Implementation Plans];
- Develop plans to validate actions as outlined in the Security Technical Implementation Guide (STIG) checklists; (CDRL A006)
- Assist Cybersecurity Analyst / Test Team Lead with evaluation Cybersecurity self-assessment results and evidence;
- Ensure Cybersecurity test procedures are available and visible for replication use across systems utilizing the same hardware and software;
- Utilize eMASS and the Defense Information System Agency's (DISA) latest vulnerability management system for the documentation of test evidence and risk assessment for each system

#### 3.6.2 Program Office RMF Support

For tasking requiring TS-SCI clearance as determined by the Government, the contractor shall provide the following support:

##### 3.6.2.1 The contractor shall provide RMF Documentation Support:

- Develop all RMF documentation in accordance with DoD/DHA policies and procedures to ensure that authorization packages are complete and system compliance accurately documented for the Authorizing Official (AO); (CDRL A006)
- Maintain Plan of Action and Milestones documentation;
- Work with the Program Management Office (PMO) to ensure that the correct RMF Process is being followed and participate in any required team meetings;
- Address authorization documentation questions from the PMO;
- Develop RMF documentation to ensure the information is current, accurate, and applicable to the article of test; (CDRL A006)
- Develop Cybersecurity self-assessment results and evidence during any Cybersecurity validation readiness reviews to determine if the system security is sufficiently mature to execute the Cybersecurity test event; (CDRL A006)
- Utilize Enterprise Mission Assurance Support Services (eMASS) and systems such as Continuous Monitoring and Risk Scoring (CMRS) for the documentation of test evidence and risk assessment for each system;
- Develop associated Cybersecurity artifacts to include, but not limited to, the System Security Plan, System Design and Architecture, Contingency Plan/Continuity of Operations Plan (COOP) Plan, Incident response Plan, Audit Design, Change Control Board, Identification and Authentication, Physical and Environmental, and Remote artifacts; (CDRL A006)
- Provide all necessary status report to the Government PM documenting the progress/results of Program Office RMF Support (CDRL A006)

#### 3.6.2.2 The contractor shall provide Self-Assessment Support:

- Work with Independent Verification & Validation (IV&V) Lead to develop test plans and participate in system related team meetings;
- Prepare for on-site self-assessments;
- Execute tests in accordance with test plans;
- Prepare test events status reports and out-briefs; (CDRL A006)
- Populate databases such as eMASS and CMRS with test results and provide input into test event reporting;
- Assemble Cybersecurity package [e.g. Scorecard, Plans of Action & Milestones (POA&M), Certification Documentation, Implementation Plans];
- Develop plans to validate actions as outlined in the Security Technical Implementation Guide (STIG) checklists; (CDRL A006)
- Assist Cybersecurity Analyst / Test Team Lead with evaluation Cybersecurity self-assessment results and evidence;



- Ensure Cybersecurity test procedures are available and visible for replication use across systems utilizing the same hardware and software;
- Utilize eMASS and the Defense Information System Agency's (DISA) latest vulnerability management system for the documentation of test evidence and risk assessment for each system

### 3.7 PRIVACY & HIPAA

#### 3.7.1 Privacy and Civil Liberties Program Management Cybersecurity Compliance

3.7.1.1 Perform initial and periodic health information privacy risk assessments and conduct related ongoing compliance monitoring activities in coordination with applicable Service. Report findings as required (A007);

3.7.1.2 Interface with program Lead on Privacy items to include training and Breaches;

3.7.1.3 Develop, implement and maintain policies and procedures related to the privacy requirements of health information and related security components as outlined in the HIPAA Privacy and Security regulations and the DoD Health Information Privacy Regulation (DoD 6025.18- R) (CDRL A007);

3.7.1.4 Maintain current knowledge of, and compliance with, applicable federal and state privacy laws, accreditation standards, and applicable DoD, Service, and local facility regulations;

3.7.1.5 Monitor advancements of emerging privacy technologies to ensure that the facility is positioned to adapt and comply with these advancements;

3.7.1.6 Evaluate industry best practices related to the privacy of health information. Incorporate these best practices, where possible, into facility operations;

3.7.1.7 Monitor Business Associate Agreements related to privacy concerns;

#### 3.7.2 Cybersecurity Compliance for HIPAA - works with Privacy and Civil Liberties Office on PIA and SORN requirements;

3.7.2.1 Maintain and update all required HIPAA compliance documentation as outlined in the HIPAA Privacy Rule and DoD regulations;

3.7.2.2 Interface with program lead on HIPAA items to include training and breaches;

3.7.2.3 Ensure that privacy related policies and procedures are reviewed for accuracy at a minimum, annually, or more often if there is a material change to a HIPAA privacy standard or requirement, MHS privacy requirement, or local business practice;

3.7.2.4 Perform initial and periodic health information privacy risk assessments and conduct related ongoing compliance monitoring activities in coordination with applicable Service. Report findings as required (CDRL A007);

3.7.2.5 Ensure a mechanism is in place within the facility for receiving, documenting, tracking, investigating, and responding to all privacy-related complaints. Coordinate these actions with other pertinent functional areas within the facility. Consult with legal counsel, as necessary;

3.7.2.6 Maintain and update all required HIPAA compliance documentation as outlined in the HIPAA Privacy Rule and DoD regulations;

3.7.2.7 Establish metrics for monitoring compliance with HIPAA privacy standards. Provide these results to senior facility leadership and higher authority within the program, as requested.

### 3.8 TECHNICAL SUPPORT

#### 3.8.1 Cybersecurity Documentation and Reports

The contractor shall be able to apply the Cybersecurity disciplines required to ensure that the technical support community is provided with adequate instruction including applied exercises resulting in the attainment and retention of knowledge, skills, attitudes, and subject matter expertise regarding applicable Cybersecurity systems. Contractor shall develop presentations, reports, white papers, and training documentation as required.(A001)

### 3.9 EQUIPMENT AND MATERIAL SUPPORT

#### 3.9.1 Procurement Support

The contractor shall research and procure/fabricate equipment and/or material in support of the performance requirements. Under this cost reimbursable contract line items, items purchased are known as contractor-acquired property (CAP) and are identified in PWS Para 10.2. To ensure fair and reasonable pricing under this cost reimbursable contract line item, the contractor shall ensure acquisition selection factors include price, availability, reliability, and supportability within current supply system. The contractor shall keep source selection records and make it available for government review as needed. Prior to purchasing items, the contractor shall obtain COR concurrence. The contractor shall provide all support data and cost estimates necessary to justify a fair and reasonable price per item procured. As mandated in the FAR, the contractor shall have an adequate accounting system to track all items ordered and its associated delivery status. After receipt, the contractor shall have an adequate property management system to track each item location. All items procured by the contractor shall be utilized or staged at the contractor's facility transported by the contractor to the installation, integrated or consumed in a system, or returned to the government at the completion of the task order. The contractor shall be responsible for managing Government property in accordance with PWS Para 10.3. Contractor shall recommend and procure items that conform to the following applicable product validation, identification, and tracking requirements.

3.9.1.1 Product Validation – The contractor shall certify that it purchases supplies from authorized resellers and/or distributors. The contractor shall warrant that the products are new, in their original box. The contractor shall obtain all manufacturer products submitted in task order offers from authentic manufacturers or through legal distribution channels only, in accordance with all applicable laws and policies at the time of purchase. The contractor shall provide the Government with a copy of the End User license agreement, and shall warrant that all manufacturer software is licensed originally to Government as the original licensee authorized to use the manufacturer software. The contractor shall track the licensing information and have it available for government review.

3.9.1.2 IT Security Requirements – The contractor shall ensure that all products recommended and/or procured meet cybersecurity and computer requirements specified in PWS Para 4.0.

3.9.1.3 Electronic Parts – In order to mitigate use of counterfeit and/or defective electronic parts, the contractor shall ensure all acquired electronic parts comply with the notification, inspection, testing, and authentication requirements in accordance with DFARS 252.246-7007 DFARS 252.246-7008 specific to electronic parts.

3.9.1.4 Item Unique Identification (IUID) – In accordance with SECNAVINST 4440.34, the contractor shall ensure that certain delivered items manufactured, integrated, or purchased (depending if item meets a unit cost threshold, is serially managed, or if government specifies identification

required) have an item unique identification or Unique Item Identifier (UII). If specified by the Government, prior to delivery, the contractor shall clearly mark and identify each applicable item based on the guidance provided in DoD MIL-STD-130N for those items not already marked. With Government concurrence, the contractor shall specify the construct, syntax, marking methodology, and quality methodology chosen to mark the required parts and any corresponding technical justification. All IUID information shall be recorded and shall be subject to Government review. The contractor shall track IUID items and maintain information being recorded. Prior to delivery of applicable CAP item, the contractor shall register items with Unique Item Identifier (UII) in the IUID Registry.

### 3.10 GOVERNMENT CONTROLLED COMPUTER ASSETS

In the performance of this work, the contractor shall furnish compatible computing platforms as an indirect cost for each employee executing tasking under section 3.0 that is capable of exclusively running the secure software image furnished under section 9.0. The contractor shall enable the Government to install this software image on the computing hardware and allow the Government to subsequently maintain the secure software image such that the computing hardware running it will be referred to as Government Controlled Equipment (GCE). The Hardware APL list, Attachment #3, provides the contractor with the minimum specifications of the required computing platforms.

#### 3.10.1 Hardware Maintenance

The contractor shall maintain ownership of the computing hardware on the contractor furnished laptops and as such shall maintain the hardware platform to include replacement of the platform due to equipment breakage or malfunction. The contractor shall also provide upgraded hardware on the contractor furnished laptops as necessary to support upgrades to the Government furnished computing image as required. At the end of the contract, or during performance where GCE is removed from service or replaced by the contractor, the contractor shall make arrangements for the Government to remove the secure computing image and Government data from all contractor owned computing hardware before it is returned to the contractor for their final disposition.

#### 3.10.2 Tracking and Reporting

The contractor shall use Government-provided computing platform image (see section 9.0, Item #1) on all contractor-owned computer assets supporting this task order. Contractor personnel shall arrange with Government personnel for computer assets to be loaded with appropriate software. During the task order performance, the contractor shall track all computer assets with the Government-provided platform image and report in the monthly task order status report the quantities and location of each asset. In the event the asset is damaged/unfixable, no longer needed, or at the completion of the task order, the contractor shall arrange with the appropriate Government personnel for each asset to be cleaned/erased of all Government provided software and platform images. In the event a Government controlled asset is lost or stolen, the contractor shall notify the COR verbally and in writing no later than 24 hours from the time the asset is known missing.

### 3.11 OFFSHORE PROCUREMENT OF COMSEC EQUIPMENT

Due to the unique sensitivity of Communications Security and to maintain rigid control over the integrity of COMSEC equipment, the contractor shall not award any subcontracts or purchase orders which involve design, manufacture, production, assembly or test in a location not in the United States, of equipment, assemblies, accessories or parts performing cryptographic functions under this contract without prior specific approval of the Contracting Officer. The contractor shall include this text in any and all subcontracts that are issued in support of this task order for equipment, assemblies, accessories or parts.

## **4.0 INFORMATION TECHNOLOGY (IT) SERVICES REQUIREMENTS**

### **4.1 INFORMATION TECHNOLOGY (IT) GENERAL REQUIREMENTS**

The contractor shall adhere to the following requirements when the IT support services and/or supply are applicable to the requirement:

- 4.1.1 Ensure that no production systems are operational on any research, development, test and evaluation (RDT&E) network.
- 4.1.2 Follow DoDI 8510.01 when deploying, integrating, and implementing IT capabilities.
- 4.1.3 Migrate all Navy Ashore production systems to the Navy, Marine Corps Intranet (NMCI) environment where available.
- 4.1.4 Work with Government personnel to ensure compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).
- 4.1.5 Follow SECNAVINST 5239.3C and DoDI 8510.01 prior to integration and implementation of IT solutions or systems.
- 4.1.6 Register any contractor-owned or contractor-maintained IT systems utilized on task order in the Department of Defense IT Portfolio Registry (DITPR)-DON.
- 4.1.7 Ensure all IT products and services recommended, procured, and/or developed is compliant with Section 508 of the Rehabilitation Act of 1973, Title 36 Code of Federal Regulations Part 1194 – Electronic and Information Technology Accessibility Standards unless otherwise exempt in accordance with the latest regulation.
- 4.1.8 Only perform work specified within the limitations of the basic contract and task order.
- 4.2 **ACQUISITION OF COMMERCIAL SOFTWARE PRODUCTS, HARDWARE, AND RELATED SERVICES**

Contractors recommending or purchasing commercial software products, hardware, and related services that support Navy or DoD programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

4.2.1 DoN Enterprise Licensing Agreement/DoD Enterprise Software Initiative Program  
Pursuant to DoN Memorandum – Mandatory use of DoN Enterprise Licensing Agreement (ELA), contractors that are authorized to use Government supply sources per FAR Subpart 51.101 shall verify if the product is attainable through DoN ELAs and if so, procure that item in accordance with appropriate ELA procedures. If an item is not attainable through the DoN ELA program, contractors shall then utilize DoD Enterprise Software Initiative (ESI) program as prescribed in DFARS Subpart 208.74 and Government-wide SmartBuy program (see DoD memo dtd 22 Dec 05). The contractor shall ensure any items purchased outside these programs have the required approved waivers as applicable to the program. The contractor shall purchase the following software and/or software license(s):

#### **BASE YEAR**

<b>Item #</b>	<b>Description</b>	<b>Unit/Issue</b>	<b>Quantity</b>
1	Camtasia	Ea	3

FOR EACH OPTION YEAR, IF EXERCISED

[Ver dtd June 25]

Item #	Description	Unit/Issue	Quantity
1	Camtasia	Ea	3

#### 4.2.2 DoN Application and Database Management System (DADMS)

The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DoN Application and Database Management System (DADMS) and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. The RDT&E network does not provide continuous support to operational entities. The contractor shall ensure that any system achieving operation fleet readiness and support is removed from the RDT&E environment and hosted on the respective enterprise solution as required. The contractor shall ensure any systems or applications integrated, installed, or operated on the RDT&E network must be in accordance with DADMS and/or DITPR-DON registration policies. Exemptions to this policy can apply as specified by higher directives. Exemptions on systems that remain on the RDT&E are normally systems that support the RDT&E or have to be on the RDT&E to achieve their target of support.

#### 4.2.3 Cybersecurity/Computer Security Requirements

The contractor shall ensure that all products recommended and/or procured that impact cybersecurity shall be selected from the National Information Assurance Partnership (NIAP) Validated Products List. The contractor shall ensure the products chosen are based on the appropriate NIAP-approved Protection Profile (PP) for the network involved and are utilized in accordance with latest Defense Information Systems Agency (DISA) policy at time of order. The contractor shall store all product information and have it available for government review at any time.

#### 4.2.4 Supply Chain Risk Management

“Covered item of supply” (e.g., software, processor, etc.) is any information technology item that is purchased for inclusion in a “covered system” (i.e., national security systems). In accordance with DFARS 252.239-7018, the contractor shall have mechanisms in place to effectively monitor the supply chain for critical components, understands how supply chain risk can be introduced through those components, and shall have implemented or plans to implement countermeasures to mitigate the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

### 4.3 CYBERSECURITY SUPPORT

Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DoN cybersecurity requirements.

#### 4.3.1 Cyber IT and Cybersecurity Personnel

4.3.1.1 The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS 252.239-7001, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoDM 8140.03, Cyberspace Workforce Qualification and Management

Program. Proposed contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the task order performance period or before assignment to the task order during the course of the performance period.

4.3.1.2 Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete the latest System Authorization Access Request (SAAR) DD Form 2875 as needed to qualify for a common access card (CAC).

4.3.1.3 Contractor personnel with privileged access shall have a favorably adjudicated Tier 5 (or DoD equivalent) background investigation in accordance with SECNAVINST 5510.30C and acknowledge special responsibilities with a Privileged Access Agreement (PAA) in accordance with SECNAVINST 5239.20A.

4.3.1.4 The contractor shall ensure compliant Cyber IT and Cybersecurity personnel are entered into the Defense Eligibility Enrollment System (DEERS) or another appropriate database. Contractor personnel who fail to maintain their certified status or favorable adjudication will not be permitted to carry out the responsibilities of the position. The contractor shall replace unqualified personnel with individuals who meet the minimum certification requirements as mandated by DoD.

#### 4.3.2 Design, Integration, Configuration or Installation of Hardware and Software

The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01. The contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DoN cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum: Acceptable Use of Department of the Navy Information Technology (IT) dtd 12 Feb 16. Use of blacklisted software is specifically prohibited and only software that is registered in DON Application and Database Management System (DADMS) and is Functional Area Manager (FAM) approved can be used as documented in Para 4.2 when applicable. Procurement and installation of software governed by DON Enterprise License Agreements (ELAs) – Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DON CIO Policy and DON ELAs awarded.

#### 4.3.3 Cybersecurity Workforce (CSWF) Report

Pursuant to DFARS 252.239-7001, the contractor shall identify cybersecurity personnel, also known as CSWF and Cyber IT workforce personnel in accordance with DoDM 8140.03. The contractor shall develop, maintain, and submit a monthly CSWF Report (CDRL A008) identifying CSWF individuals who are cybersecurity trained and certified. Utilizing the format provided in the data item description (DID) DI-MGMT-82160, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DoD (DD) Form 1423 for additional reporting details and distribution instructions. Although the minimum frequency of reporting is monthly, the COR can require additional updates at any time. The contractor shall verify with the COR or another Government representative the proper labor category CSWF designation and certification requirements. The contractor shall ensure CSWF personnel meet the minimum cyber security training and certification requirements in accordance with the latest DoD Information Assurance/Cyberspace Workforce manual. The primary point of contact (POC) for all related CSWF questions is the Command CSWF Program Manager (PM) in the office of the NIWC Atlantic Information Systems Security Manager (ISSM).

#### 4.3.4 Cybersecurity Workforce (CSWF) Designation

CSWF contractor personnel shall perform cybersecurity functions and shall meet the requirements in accordance with DoDM 8140.03 Para 3.1.a-d and 3.2.

## 5.0 TASK ORDER ADMINISTRATION

Government monitoring to ensure contracted services are being performed is an administrative requirement. The contractor shall provide support and documentation as required to ensure adequate monitoring and management can be performed. The objective of the contractor is ensuring the Government's requirements are met, delivered on schedule, and performed within budget.

### 5.1 CONTRACTOR LIAISON

The contractor shall assign a technical single point of contact, also known as the Program Manager (PM) who shall work closely with the Government Contracting Officer and COR. The contractor PM, located in the contractor's facility, shall ultimately be responsible for ensuring that the contractor's performance meets all Government contracting requirements within cost and schedule. PM shall have the requisite authority for full control over all company resources necessary for task order performance and be available to support emergent situations. The PM shall ultimately be responsible for the following: personnel management; management of Government material and assets; and personnel and facility security. In support of open communication, the contractor shall initiate periodic meetings with the COR.

### 5.2 CONTRACT MONITORING AND MAINTENANCE

The contractor shall have processes established in order to provide all necessary resources and documentation during various times throughout the day including business and non-business hours in order to facilitate a timely task order response or modification in particular during urgent requirements. Various types of administrative documents are required throughout the life of the task order. At a minimum, the contractor shall provide the following documentation:

#### 5.2.1 Task Order Status Report (TOSR)

The contractor shall develop a Task Order Status Report (TOSR) (CDRL A009) and submit it monthly; the initial report is due at least 30 days after task order award and on the 10<sup>th</sup> of each month for those months the task order is active. The prime contractor shall be responsible for collecting, integrating, and reporting any subcontractor reports. This CDRL includes the completion of applicable attachment(s) as cited in the DD Form 1423. The contractor shall deliver the TOSR in an editable format; see applicable DD Form 1423 for additional reporting details and distribution instructions.

#### 5.2.2 Weekly Status Report

The contractor shall develop and submit a weekly status report (CDRL A00A) which is e-mailed to the COR no later than close of business (COB) every Friday. The first report is required on the first Friday following the first full week after the task order award date. The contractor shall ensure the initial report includes a projected Plan Of Action and Milestones (POA&M). At a minimum, the contractor shall include in the weekly report the following items and data:

1. Percentage of work completed
2. Percentage of funds expended per ship/sub/shore command and system
3. Updates to the POA&M and narratives to explain any variances

#### 5.2.3 Data Call/Ad-hoc Status Report

The contractor shall develop and submit a data call report (CDRL A00B) which is e-mailed to the COR within six working hours of the request. The contractor shall ensure all information provided is the most current. Cost and funding data will reflect real-time balances. Report will account for all planned, obligated, and expended charges and hours. At a minimum, the contractor shall include in the data call the following items and data:

1. Percentage of work completed
2. Percentage of funds expended

3. Updates to the POA&M and narratives to explain any variances
4. List of personnel (by location, security clearance, quantity)
5. Most current GFP and/or contractor acquired Property (CAP) listing

#### 5.2.4 Electronic Cost Reporting and Financial Tracking (eCRAFT)

The contractor shall complete an Electronic Cost Reporting and Financial Tracking (eCRAFT) Report (CDRL A00C) and submit the report on the day and for the same timeframe as when the contractor submits an invoice into the Wide Area Workflow (WAWF) module on the Procurement Integrated Enterprise Environment (PIEE) system. The data reported in eCRAFT Periodic Reporting Utility (EPRU) spreadsheet shall correspond to the data reported in WAWF. Compliance with this requirement is a material requirement of this contract/order. Failure to comply with this requirement may result in contract/order termination. The contractor shall refer to the applicable eCRAFT labor category in the Section C Personnel Qualification requirements and review DD Form 1423 for reporting details and upload instructions.

#### 5.2.5 Closeout Report

The contractor shall develop a task order closeout report (CDRL A00D) and submit it no later than 15 days before the task order completion date to allow for any corrective actions. The prime contractor shall be responsible for collecting, integrating, and reporting all subcontracting information, if applicable. See corresponding DD Form 1423 for additional reporting details and distribution instructions. The contractor shall ensure with the COR no corrective action is identified, and if corrective action is necessary, the contractor shall rectify issue prior to the end of task order performance period.

### 5.3 PERFORMANCE MANAGEMENT

Contractor performance standards and requirements are outlined in the task order QASP. The ability of a contractor to perform to the outlined standards and requirements will be captured in the Contractor Performance Assessment Reporting System (CPARS). In support of tracking contractor performance, the contractor shall provide the following documents: Cost and Schedule Milestone Plan (CDRL A00E) submitted 10 days after task order award and CPARS Draft Approval Document (CDAD) Report (CDRL A00F) submitted monthly.

### 5.4 RESOURCE MANAGEMENT

The contractor shall ensure all personnel, including subcontracted personnel, can perform the applicable tasking as outlined in the associated contract/order PWS in an efficient, reliable, and professional manner while maintaining applicable personnel qualifications, certification and/or training, and security clearance requirements. The ability of a contractor to provide resources in accordance with the standards and requirements will be captured in the Contractor Performance Assessment Reporting System (CPARS).

(a) Applicable labor categories (LCATs) consist of either the Electronic Cost Reporting and Financial Tracking (eCRAFT) Professional Categories and/or Standard Contract Labor Standards (SCLS) in accordance with the Service Contract Act (SCA) Directory of Occupations.

(b) The Government reserves the right to review resumes of contractor personnel as required during performance of the contract/order.

(c) If the Government questions the qualifications or competence of any persons performing under the contract/order, the burden of proof to sustain that the persons is qualified as prescribed herein shall be upon the contractor.



(d) The contractor shall have personnel, organization, and administrative control necessary to ensure that the services performed meet all requirements specified in contract/orders. The work history of each contractor employee shall contain experience directly related to the tasks and functions to be assigned. The Government reserves the right to determine if a given work history contains necessary and sufficiently detailed, related experience to reasonably ensure the ability for effective and efficient performance.

(e) The contractor shall apply the following criteria when validating education and experience requirements:

i. Postsecondary education: Associate of Art (AA), Associate of Science (AS), Bachelor of Science (BS), Bachelor of Arts (BA), Master's (MS), and Doctor of Philosophy (PhD) shall meet an acceptable level of quality and integrity; acceptable educational degrees shall be earned from accredited institutions or programs as cited by the U.S. Department of Education ([www.ed.gov](http://www.ed.gov)). The contractor shall ensure the postsecondary education earned by their employees meets accreditation requirements and not accredited by a fraudulent accrediting body. At a minimum, Bachelor of Science (BS), Bachelor of Arts (BA), Master (MS), and Doctorate (PhD) degrees shall come from institutions that are regionally accredited at the same time the degree was earned. For education earned outside of the United States, the contractor shall ensure the education is equivalent to education gained in a conventional/accredited U.S. program. Degrees received abroad shall be reviewed by a U.S. based credential evaluation service which must be cited in the applicable employee's resume.

ii. Engineering Positions require diploma/written engineering degrees versus grandfathered degrees based on experience. If a state Professional Engineer (PE) License, training certification, and/or license is required for the performance of the requirement, the government will specify any unique certifications or license under the applicable LCAT personnel qualification. Technology degrees (i.e., associate's degrees or trade-related degrees) do not qualify as Engineering or Physical Science Degrees.

iii. Unless otherwise specified, higher education (i.e., graduate degree) above a labor category's typical requirement can be credited as years of experience if the higher degree is within the same required field of study as the minimum degree required. The following educational credit applies: a Master's degree equals four (4) years of experience, and a Doctoral degree equals five (5) years of experience; no substitution is allowed for Bachelor's degrees unless specified within the applicable labor category.

#### 5.4.1 Non-Key Personnel

Throughout the task order period of performance, the contractor shall provide qualified non-Key Personnel for applicable labor categories to support this contract/order in accordance with the labor category descriptions identified at the following Naval Undersea Warfare Center (NUWC) Division Newport public website link: <https://www.navsea.navy.mil/Home/Warfare-Centers/NUWC-Newport/Partnerships/Commercial-Contracts/Labor-Categories/>.

#### 5.4.2 Key Personnel

In addition to the personnel qualifications outline within the NUWC Division Newport website, throughout the task order period of performance, the contractor shall provide Key Personnel that meet the following personnel qualifications.

##### **1. Manager, Program/Project II**

**(eCRAFT code: MANP2)**

**Special Experience:** Four (4) years as manager of information assurance or computer network defense projects. Experience may be achieved simultaneously.

## 2. Manager, Program/Project III

(eCRAFT code: MANP3)

**Special Experience:** Five (5) years as manager of information assurance or computer network defense projects. Experience may be achieved simultaneously.

(a) The contractor agrees to assign key personnel to this contract/order listed in paragraph (d) below. Within 90 days after contract/order award, the contractor shall submit resumes for each of the key labor categories listed. After approval, the individuals shall be added to a key personnel list, paragraph (d), which shall be maintained by the contractor and supplied in the monthly CSR/TOSR CDRL. No substitutions shall be made except in accordance with this text.

(b) The contractor shall not initiate any personnel substitutions during the first 120 days of the contract/order performance period unless such substitutions are necessitated by an individual's sudden illness, death, or termination of employment. In any of these events, the contractor shall promptly notify the Contracting Officer and provide the information required by paragraph (c) below. After the initial 120-day period, all proposed substitutions shall be submitted in writing, at least fifteen (15) days (thirty (30) days if a security clearance is obtained) in advance of the proposed substitutions to the Contracting Officer. The contractor shall include with each substitution request the information required by paragraph (c) below.

(c) The contractor shall provide all requests for approval of substitutions under this contract/order in writing which includes a detailed explanation of the circumstances necessitating the proposed substitutions. The request must contain a complete resume for the proposed substitute or addition, and any other information requested by the Contracting Officer is necessary to approve or disapprove the proposed substitutions. All substitutions proposed during the duration of this contract/order must have the qualifications of the person being replaced. The Contracting Officer or his authorized representative will evaluate such requests and promptly notify the contractor of his approval or disapproval thereof in writing.

(d) List of Key Personnel – The contractor shall track and maintain a Key Personnel Listing which shall be submitted as part of the regularly scheduled contract/task order status report.

<b>CONTRACT LABOR CATEGORY</b>
MANAGER, PROGRAM/PROJECT II
MANAGER, PROGRAM/PROJECT III
ENGINEER, CYBERSECURITY III (Team Lead KEY)
SPECIALIST, QUALITY CONTROL IV (Team Lead KEY)

(e) If the Contracting Officer determines that suitable and timely replacement of key personnel is not reasonably forthcoming or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract/order, the Contracting Officer may terminate the contract for default or for the convenience of the Government, as appropriate. In addition, if the contractor is found at fault for the condition, the Contracting Officer may elect to equitably decrease the contract price or fixed fee to compensate the Government for any resultant delay, loss, or damage. The contractor's ability to manage, provide, and/or maintain sufficient key personnel will be evaluated in the annual government Contractor Performance Assessment Report (CPAR) rating.

(f) If the contractor wishes to add personnel to be used in a labor category, the contractor shall employ the procedures outlined in paragraph (c) above.

### 5.5 EARNED VALUE MANAGEMENT (EVM)

In accordance with DoD policy, this task order does not require Earned Value Management (EVM) implementation due to the majority of efforts on this task order is non-scheduled based (i.e., level of effort) and does not lend itself to meaningful EVM information. In lieu of an EVM system, the

contractor shall develop and maintain a Contract Funds Status Report (CDRL A00G) to help track cost expenditures against performance.

## 6.0 DOCUMENTATION AND DELIVERABLES

### 6.1 CONTRACT DATA REQUIREMENTS LIST (CDRL)

The following listing identifies the data item deliverables required under this task order and the applicable section of the PWS for which they are required. Section J includes the DW Form 1423s that itemize each Contract Data Requirements List (CDRL) required under this task order. The contractor shall establish a practical and cost-effective system for developing and tracking the required CDRLs. The contractor shall not develop any CDRL classified TOP SECRET with Sensitive Compartmented Information (SCI).

Unless otherwise specified, dates are calendar days; one week equals 7 calendar days; 1 days equals 24 hours; and a 24-hour time period is consecutive hours that is exclusive of non-workweek days.

#### 6.1.1 Administrative CDRL

The following table lists all required administrative data deliverables, CDRLs, applicable to this task:

CDRL #	Deliverable Title (& Subtitle, if applicable)	PWS Reference Para	Frequency	Date Due	Security Classification (up to Secret, Top Secret or unclassified)
A008	Cybersecurity Workforce (CSWF) Report	4.3.3, 8.1.2, 8.2.3.1	MTHLY	30 Days after task order award (DATO) and monthly on the 10th	Unclass
A009	Contract Status Report: Task Order Status Report (TOSR)	5.2.1, 8.1.2, 8.2.2.3(c), 8.2.3.1, 10.3.3, 10.3.3.1	MTHLY	30 DATO and monthly on the 10th	Unclass
A00A	Contract Status Report: Weekly Status Report	5.2.2	WKLY	Every Friday after 7 days of task order award	Unclass
A00B	Contract Status Report: Data Call	5.2.3	ASREQ	Within 24-48 hrs after request	Unclass
A00C	Contract Status Report: Electronic Cost Reporting and Financial Tracking (eCRAFT) Report	5.2.4	ASREQ	Same date when invoice is submitted to WAWF	Unclass
A00D	Contract Status Report: Closeout Report	5.2.5, 8.2.2.3 (c), 10.3.7	1TIME	NLT 15 days before completion date	Unclass
A00E	Performance and Cost Report: Cost and Schedule Milestone Plan	5.3	One time with	NLT 10 DATO; revision NLT 7	Unclass

CDRL #	Deliverable Title (& Subtitle, if applicable)	PWS Reference Para	Frequency	Date Due	Security Classification (up to Secret, Top Secret or unclassified)
			revisions (ONE/R)	days after receipt of Govt review	
A00F	Performance and Cost Report: Contractor CPARS Draft Approval Document (CDAD) Report	5.3	MTHLY	30 DATO and monthly on the 10 <sup>th</sup>	Unclass
A00H	Management Plan: Mitigation Plan	8.2.4.6	One time with revisions (ONE/R)	NLT 45 days following execution of NDA; revision NLT 14 days after receipt of Govt review	Unclass

#### 6.1.2 Technical CDRL

The following table lists all required technical data deliverables, (CDRLs), applicable to this task order:

CDRL #	Deliverable Title	PWS Ref Para	Frequency	Date Due	Security Classification (up to Secret, Top Secret or unclassified)
A001	Program Management Reports	3.2.2, 3.4.1.4, 3.4.2.4, 3.5.3, 3.8.1	ASREQ	Within 5 business days from request	Up to TS
A002	Weekly System Status Report	3.2.2	WKLY	Every Wednesday	Unclass
A003	Travel and Leave Tracker	3.2.2	WKLY	Every Monday	Unclass
A004	Cost Estimate For System/Enclave	3.2.2	ASREQ	Within 24 hrs from request	Unclass
A005	Available Budget and Expensed Funding at System/Enclave Level	3.2.2	MTHLY	30 DATO and monthly on the 10th	Unclass
A006	RMF Documentation	3.3.1.1, 3.3.2.1, 3.3.1.3, 3.3.2.3, 3.4.1.1, 3.4.1.2, 3.4.1.4, 3.4.1.5,	ASREQ	Within 5 business days from request	Up to TS

CDRL #	Deliverable Title	PWS Ref Para	Frequency	Date Due	Security Classification (up to Secret, Top Secret or unclassified)
		3.4.1.6, 3.4.1.7, 3.4.2.1, 3.4.2.2, 3.4.2.4, 3.4.2.5, 3.4.2.6, 3.4.2.7, 3.6.1.1, 3.6.1.2, 3.6.2.1			
A007	Privacy/HIPPA Reports	3.7.1.1, 3.7.1.3, 3.7.2.4	ASREQ	Within 5 business days from request	Unclass
A00G	Contract Funds Status Report (CFSR)	5.5	Monthly	10 <sup>th</sup> of Each Month	Unclass

## 6.2 ELECTRONIC FORMAT

### 6.2.1 Deliverable Format

The contractor shall ensure all CDRLs, data, correspondence, and etc. are provided in a format approved by the COR/receiving Government representative. Unless otherwise specified, the contractor shall provide all data in an editable format compatible with NIWC Atlantic corporate standard software configuration as specified below. Hard copies requirements will be specified within the applicable CDRL requirements. Contractor shall conform to NIWC Atlantic corporate standards within 30 days of task order award. *The initial or future upgrades costs of the listed computer programs are not chargeable as a direct cost to the Government.*

	Deliverable	Software to be used
a.	Word Processing	Microsoft Word
b.	Spreadsheet/Graphics	Microsoft Excel
c.	Presentations	Microsoft PowerPoint
d.	2-D Drawings/ Graphics/Schematics (existing data products)	Raster (CALS Type I, TIFF/BMP, JPEG, PNG)
e.	Scheduling	Microsoft Project
f.	On-line Training Development	Adobe Captivate

### 6.2.2 Deliverable Reporting

Deliverable requirements are set forth within the applicable PWS paragraphs and within each CDRL DD1423. The contractor shall upload appropriate non-classified deliverable documents to the Acquisition Management System (AMS) CDRL Tool:

<https://ams.navair.navy.mil/CDRL/Pages/Default.aspx>. In the event reporting to AMS inhibits the receipt of the deliverable to the Government, the contractor shall forward the deliverable directly to the COR through email or as directed for documents with submission restrictions.

## 6.3 INFORMATION SYSTEM COMMUNICATION

### 6.3.1 Compatibility

The contractor shall have broadband Internet connectivity and an industry standard email system for communication with the Government. The contractor shall be capable of Public Key Infrastructure (PKI) client side authentication to DOD private web servers. Unless otherwise specified, all key personnel on task shall be accessible by e-mail through individual accounts during all hours. The contractor shall have an information system (IS) capable of meeting all security requirements identified under Para 8.4.

#### 6.3.2 Accessibility

The contractor shall upload appropriate unclassified deliverable documents to the Acquisition Management System (AMS). Prior to CDRL submission due date, the contractor shall establish necessary access to the Government IS (i.e., AMS and Product Data Reporting and Evaluation Program (PDREP) website that is required for eCRAFT reporting) by utilizing an employee issued Common Access Card (CAC) and/or DoD approved External Certification Authority (ECA) (<https://public.cyber.mil/eca/>). For AMS access, the contractor shall ensure they establish "Contractor" roles within the AMS CDRL Tool. No later than 10 days after task order award, the contractor shall notify the COR they have successfully created an AMS account so that proper Contractor Permissions can be assigned.

#### 6.3.3 Communications Restriction

The contractor shall meet the security control requirements for processing, storing and transmitting Controlled unclassified information (CUI). The contractor shall evaluate every deliverable for either CUI or classified information using the applicable program Security Classification Guide and assign the correct classification and apply CUI-Controlled Technical Information (CTI) markings in accordance with DoDI 5200.48 (CUI) and DoDI 5230.24 (CTI) as applicable. The contractor shall not upload deliverables that contain restricted program CTI or classified information to AMS. The contractor shall deliver these documents to the COR via one of the three methods as directed in the appropriate PWS task or by the COR:

- (1) send by Secure Internet Protocol Router Network (SIPRNet) email
- (2) delivered by DOD SAFE on SIPRNet
- (3) posted to the IPT's SIPRNet SharePoint site

When submitting deliverables containing restricted CTI or classified information outside of AMS, the contractor shall send a sanitized (i.e. containing no CTI or classified information) notification indicating the document has been delivered to the COR. The contractor shall upload a cover sheet to AMS within the due date of the CDRL containing the following minimum information:

- Contractor Name
- Contract Number
- Task/Delivery Order Number
- CDRL Number
- CDRL Title and Subtitle, if applicable (in accordance with DD1423)
- Status: Draft/Final
- Date Submitted on SIPRNet
- Method of SIPRNet submission (SIPRNet email, posted, DOD SAFE)
- Name of contractor personnel responsible for submission content
- Name of contractor personnel responsible for submission delivery/upload

## 7.0 **QUALITY**

### 7.1 **MANAGE QUALITY COMPLIANCE**

#### 7.1.1 General

The contractor shall have quality processes or Quality Management System (QMS) processes in place that coincide with the Government's Manage Quality processes which address Quality Control, Quality Assurance, Software Quality, and/or project Quality System tasks. The contractor shall use

best industry practices including, when applicable, ISO/IEC 15288:2015 for System life cycle processes and ISO/IEC 12207:2017 for Software life cycle processes. As applicable, the contractor shall also support and/or participate in Acquisition Milestones, Phases, and Decision Points, which are standard elements of the Defense Acquisition System and support DoDD 5000.01 and DoDI 5000.02. The contractor shall provide technical program and project management support that will mitigate the risks to successful program execution including employment and objective evidence of Lean Six Sigma, Risk Management, and System Engineering methodologies; and System and Software Engineering best practices. As part of a team, the contractor shall support projects at NIWC Atlantic that are currently, or in the process of, being assessed under a Capability Maturity Model Integration (CMMI) program. The contractor shall be required to utilize the processes and procedures already established for the project and deliver products that are compliant with the aforementioned processes and procedures that is commensurate with the CMMI level the government project is at or working towards. Contractor is not required to have a formal CMMI appraisal; however, possession is desired.

## 7.2 QUALITY ASSURANCE

The contractor shall perform all quality assurance process audits necessary in the performance of the various tasks as assigned and identified in the contractor's Quality Assurance Plan (QAP) or by the respective WBS, POA&M, or quality system/QMS documentation in support of continuous improvement. The contractor shall deliver related QAP and any associated procedural documents upon request. The Government reserves the right to perform any additional audits deemed necessary to assure that the contractor processes, products, and related services, documents, and material meet the prescribed requirements and to reject any or all processes or related products, services, documents, and material in a category when noncompliance is established.

## 7.3 QUALITY CONTROL

The contractor shall perform all quality control inspections necessary in the performance of the various tasks as assigned and identified in the contractor QAP or by the respective WBS, POA&M, or quality system/QMS documentation. The contractor shall have the following related quality objective evidence available for Government review:

- (i) Detailed incoming receipt inspection records
- (ii) First article inspection records
- (iii) Certificates of Conformance
- (iv) Detailed sampling inspection records based upon MIL-STD-1916 (Verification Level III)
- (v) Quality Measurement and Analysis metrics/data

The Government reserves the right to perform any inspections or pull samples as deemed necessary to assure that the contractor provided services, documents, material, and related evidence meet the prescribed requirements and to reject any or all services, documents, and material in a category when nonconformance is established.

## 8.0 SECURITY

### 8.1 ORGANIZATION

#### 8.1.1 Security Classification

As specified in the DoD Contract Security Classification Specification, DW Form 254, the contractor shall perform classified work under this task order. At time of task order award, the contractor shall have a TOP SECRET (TS) facility clearance (FCL) with Sensitive Compartmented Information (SCI) access (TS/SCI).

8.1.1.1 U.S. Government security clearance eligibility is required to access and handle classified and certain controlled unclassified information (CUI), attend program meetings, and work within restricted areas unescorted. Access to SCI is limited to U.S. Government Facilities or other U.S. Government-sponsored controlled space as authorized on the DD254. The contractor shall not generate any SCI deliverables.

8.1.1.2 Various levels of vetting can exist to support specific PWS tasks. The following table outlines the highest (up to) required security clearance level; also, to assist in the FCL requirement to support the associated tasks of Secret and Top Secret, as applicable.

Required Security Clearance	PWS Task Paragraph
Secret	3.1, 3.2, 3.3.1, 3.4.1, 3.5, 3.6.1, 3.7, 3.8
Top Secret/SCI	3.3.2, 3.4.2, 3.6.2
None required	3.9, 3.10, 3.11

#### 8.1.2 Security Officer

The contractor shall appoint a Facility Security Officer (FSO) to support those contractor personnel requiring clearance and/or access to Government facility/installation and/or access to information technology systems under this task order. The FSO is typically a key management person who is the contractor's main POC for security issues. The FSO shall have a U.S. Government security clearance equal to or higher than the FCL required on this task order. The FSO shall be responsible for tracking the security requirements for all personnel (subcontractors included) utilized on task order. Responsibilities include tracking all personnel assigned Government Common Access Card (CAC) and NIWC Atlantic badges (issuances and expiration dates) and entering/maintaining personnel security mandatory training information within the Staffing Plan document, which is an attachment to the task order status report (TOSR) (CDRL A009), including updating and tracking data in the CSWF Report (CDRL A008). In addition, the FSO shall monitor personnel security clearance eligibility and access in the Defense Information System for Security (DISS), and ensure personnel are enrolled and subsequently re-enrolled in continuous evaluation as required for classified contracts. The FSO shall ensure the latest NIWC Atlantic Contractor Check-in and Check-out (CICO) procedures are implemented and followed.

## 8.2 PERSONNEL

The contractor shall conform to the security provisions of Title 32 Code of Federal Regulation (CFR) Part 117 – National Industrial Security Program Operating Manual (NISPOM), SECNAVINST 5510.30C, DoDI 5200.46, DoDM 1000.13-M-V1, and the Privacy Act of 1974. Prior to any labor hours being charged on this task order, the contractor shall ensure all personnel (including administrative and subcontractor personnel) have obtained and can maintain favorable background investigations at the appropriate level(s) for access required for the task order and are certified/credentialed for the CSWF. A favorable background determination is determined by either a Tier 1 (T1) investigation, Tier 3 (T3) investigation, or Tier 5 (T5) investigation and favorable Federal Bureau of Investigation (FBI) fingerprint checks. Investigations are not necessarily required for personnel performing unclassified work who do not require access to Government installations/facilities, Government IT systems and IT resources, or NIWC Atlantic information. *Cost to meet these security requirements is not directly chargeable to task order.*

NOTE: If a final determination is made that an individual does not meet or cannot maintain the minimum-security eligibility requirements, the contractor shall permanently remove the individual from NIWC Atlantic facilities, projects, and/or programs. If an individual receives an eligibility determination such as “denied”, “revoked”, “withdrawn”, “pending”, “loss of jurisdiction”, “no determination made,” or receives unfavorable fingerprint results, the contractor shall remove the individual from NIWC Atlantic facilities, projects, and/or programs until such time as the investigation is fully adjudicated or the individual is eligible to reapply for security clearance



eligibility and/or CAC credentialing per DoDI 5200.46 and SECNAVISNT 5510.30C. All contractor and subcontractor personnel removed from facilities, projects, and/or programs shall cease charging labor hours directly or indirectly on task orders.

#### 8.2.1 Personnel Clearance

Some personnel associated with this task order shall possess a TOP SECRET personnel security clearance (PCL) for access. On a case-by case basis, TS clearances are eligible for access to SCI. These programs/tasks include, as a minimum, contractor personnel having the appropriate clearances required for access to classified data as applicable. Prior to starting work on the task, contractor personnel shall possess the appropriate security clearance eligibility via Defense Counterintelligence and Security Agency Consolidated Adjudication and Vetting Services (DCSA AVS) for the respective task and position assignment in accordance with SECNAVINST 5510.30C. Any future revision to the respective directive and instruction will be applied as a task order modification. Contractor personnel shall handle and safeguard any Controlled Unclassified Information (CUI) and/or classified information in accordance with appropriate Department of Defense, Navy, and NIWC Atlantic security regulations. The contractor shall immediately report any security incident or insider threat indicator to the NIWC Atlantic Security Management Office, the COR, and Government Project Manager.

8.2.1.1 The following labor categories do not require a minimum PCL:

<b>Labor Category</b>	<b>Required Minimum Personnel Security Clearance (PCL)</b>	<b>TS/SCI Access required (Y/N)</b>
Student	None Required	N

For Secret and/or TS-SCI PCL requirements by tasking, see para 8.1.1.2.

#### 8.2.2 Access Control of Contractor Personnel

The contractor shall facilitate the required access for each employee. The ability of the contractor to manage and maintain accessibility in accordance with the applicable requirements is captured in the annual Government CPARS rating.

##### 8.2.2.1 Physical Access to Government Facilities and Installations

Contractor personnel shall physically access Government facilities and installations for purposes of site visitation, supervisory and quality evaluation, work performed within Government spaces (either temporary or permanent), or meeting attendance. Individuals supporting these efforts shall comply with the latest security regulations applicable to the Government facility/installation.

(a) DoD Government facilities/installations require a DoD ID Card (e.g., CAC) for access. Contractor personnel shall carry proper form of identification(s) and vehicle proof of insurance or vehicle rental agreement for any liability issues. For admission to DoD installations and NIWC Atlantic facilities, all contractor personnel must have the COR or Government sponsor approved access. For contractor personnel requiring Secret or TS access, a visitor authorization request (VAR) must be submitted via Defense Information System for Security (DISS) to the Security Management Office (SMO) 652366. For access requiring a TS/SCI security clearance, the contractor shall send an additional VAR to Special Security Office (SSO) at SMO 652363.

(b) Contractor employees who make repeated deliveries to Joint Base (JB) Charleston military installations and do not require access into NIWC Atlantic facilities or DoD information system(s) shall obtain a base access card. Only contractor employees that are able to obtain a card will be eligible for entrance on base. At JB Charleston, the contractor shall obtain the required access card via the Defense Biometric Identification System (DBIDS) from the JB Charleston Badge and Pass Office. Contractors with employees that are no longer employed shall return the employee's access card directly to the COR or to the local NIWC Atlantic Security Office with COR notification within five (5) days from the last day of employment. Contractors who do not have a DBIDS card or

CAC will receive a one-day pass for each day access is required. Information about DBIDS is found at <https://dbids-global.dmdc.mil/home/>.

(c) All contractor persons engaged in work while at a Government facility/installation shall be subject to inspection of their vehicles, identification cards, and bags/parcels at any time by the Government, and shall report any known or suspected security violations to the Security Department at that location.

(d) The contractor shall notify the COR and appropriate NIWC security personnel within 24 hours from the time contractor employee gives notice of departure or are removed unexpectedly from contract support. For contractors in direct support of NIWC Atlantic, see the Contractor Check-in and Check-out (CICO) Procedures requirements listed in Para 8.2.2.5.

#### 8.2.2.2 Identification and Disclosure Requirements

All contractor and subcontractor employees located on and off Government installations shall take all means necessary to not represent themselves as Government employees. All contractor personnel shall follow the identification and Government facility disclosure requirement:

(a) Contractor employees shall be clearly identifiable as a contractor while on Government property by wearing appropriate badges.

(b) Contractor personnel and their subcontractors shall identify themselves as contractors or subcontractors during meetings, on attendance meeting list/minutes, at the beginning of telephone conversations, in electronic messages including their electronic digital signature, and all correspondence related to this task order.

(c) Contractors occupying facilities within Department of the Navy or other Government installations (such as offices, separate rooms, or cubicles) shall clearly display and identify their space with contractor supplied signs, name plates or other identification, showing that these are work areas for contractor or subcontractor personnel.

#### 8.2.2.3 Government Badge Requirements

Depending on access required, contractor personnel shall require a Government-issued picture badge. While on Government installations/facilities, contractors shall abide by each site's latest security badge requirements and prominently display (above the waist and outermost garment) their Government-issued picture badge. Government installations/facilities are continually updating their security requirements to meet Homeland Security Presidential Directive (HSPD-12) identification standards.

(a) Contractors shall submit valid paper work (e.g., site visit request, request for picture badge, etc.) to the applicable Government security office via the COR who will validate the need authorizing contractor performance within the applicable Government installation/facility.

(b) The contractor shall assume full responsibility for the proper use and security of the identification badge and is responsible for returning the badge upon termination of personnel or expiration or completion of the task order.

(c) The contractor (FSO if applicable) shall track all personnel (including subcontractors) holding CAC and/or NIWC Atlantic Government badges in support of this task as part of the TOSR (CDRL A009). At the completion of the task order, the contractor shall provide a list as part of the Closeout Report (CDRL A00D) of all returned and unreturned badges with a written explanation for any missing badges.

#### 8.2.2.4 Common Access Card (CAC) Requirements

Contractors supporting work that requires access to Government facilities/installations and/or access to any DoD IT/network also requires a CAC. Granting of logical and physical access privileges remains a local policy and business operation function of the local facility. The contractor is responsible for obtaining the latest facility/installation and IT CAC requirements from the applicable local Security Office. When a CAC is required to perform work, contractor personnel shall be able to meet all of the following security requirements prior to work being performed:

- (a) Pursuant to DoDM 1000.13-M-V1, issuance of a CAC is based on the following four criteria:
  - 1. Eligibility for a CAC – to be eligible for a CAC, Contractor personnel’s access requirement shall meet one of the following three criteria: (a) individual requires access to multiple DoD facilities or access to multiple non-DoD federally controlled facilities on behalf of the NIWC Atlantic on a recurring bases for a period of 6 months or more, (b) individual requires both access to a DoD facility and access to DoD network on site or remotely, or (c) individual requires remote access to DoD networks that use only the CAC logon for user identification.
  - 2. Verification of DoD affiliation from an authoritative data source – CAC eligible personnel must be registered in the Defense Enrollment Eligibility Reporting Systems (DEERS) through either an authoritative personnel data feed from the appropriate Service or Agency or Mission Partner Identity, Credential, and Access Management (MP ICAM).
  - 3. Completion of background vetting requirements according to FIPS PUB 201-3 and DoDI 5200.46 – at a minimum, the completion of FBI fingerprint check with favorable results and submission of a T1 investigation to the DCSA or a DoD-determined equivalent investigation. Contractor personnel shall contact the NIWC Atlantic Security Office to obtain the latest CAC requirements and procedures.
  - 4. Verification of a claimed identity – all contractor personnel shall present two forms of identification in its original form to verify a claimed identity. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1615-0047, Employment Eligibility Verification. Consistent with applicable law, at least one document from the Form I-9 list must be a valid (unexpired) State or Federal Government-issued picture identification (ID). The identity documents will be inspected for authenticity, scanned, and stored in the DEERS.
- (b) When a contractor requires logical access to a Government IT system or resource (directly or indirectly), the required CAC will have a PKI. A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official Government issued e-mail address (e.g. .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request (SAAR) form to the task order specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the NIWC Atlantic Information Systems Security Management (ISSM) office:
  - 1. For annual DoD Cybersecurity Awareness training, the contractor shall use this site: <https://twms.dc3n.navy.mil/>. For contractors requiring initial training and do not have a CAC, contact the NIWC Atlantic ISSM office at phone number (843)218-6152 or e-mail questions to niwc\_lant\_ISSMOPS.fct@us.navy.mil for additional instructions. Training can be taken at the ISSM office or online at <https://public.cyber.mil/training/cyber-awareness-challenge/>.
  - 2. Each contractor personnel shall complete a SAAR DD Form 2875. Contractors can obtain a form and shall initiate a CAC request via the latest Contractor Check-In/Check-Out procedures as posted on the NIWC Atlantic Command Operating Guide (COG) website or the NIWC Atlantic Public website at <https://www.niwcatlantic.navy.mil/workforce/Contractor-Check-In-Out/>.

#### 8.2.2.5 Contractor Check-in and Check-out (CICO) Procedures

All NIWC Atlantic contractor personnel requiring or possessing a Government badge and/or CAC for facility and/or IT access shall have a NIWC Atlantic Government sponsor and be in compliance with the most current version of Contractor Check-in and Check-out (CICO) procedures, instructions, and forms as posted on the NIWC Atlantic Command Operating Guide (COG) website or the NIWC Atlantic Public website (under “Workforce” tab, select “Contractor Check In-Out”). Each contractor employee will be assigned various IT access based on the need identified within the check-in process. In accordance with the monthly status reporting requirements, the contractor shall provide necessary employee information and documentation for employees hired, transferred, and/or terminated in support of this task order within the required timeframe as cited in the CICO instructions. The contractor (FSO, if applicable) shall have IT access to NIWC Atlantic systems for purposes of meeting CICO personnel requirement. For contractor employees whose services are no longer required, the contractor shall ensure all those employees return all applicable Government credentials (keys, CAC, site badges, tokens, etc.), any assigned Government-furnished property (e.g., laptops) are returned to the appropriate locations, and all procedures as cited in the Contractor Check-out COG page are followed which includes submitting a Check-out through the appropriate IT system(s) for each employee as applicable.

#### 8.2.2.6 Accessing Navy Enterprise Resources Planning (ERP) System

Contractor personnel shall not access the Navy Enterprise Resource Planning (Navy ERP) system.

#### 8.2.3 Mandatory Training

In addition to training and certifications requirements specified within a labor category and/or within the task support, contractor personnel (including subcontractors) shall complete applicable required mandatory training in accordance with DoD, SECNAV, and NAVWARSYSCOM directives/instructions. Pursuant to contract CICO procedures, contractor personnel will be assigned mandatory training courses when an account in Total Workforce Management System (TWMS) is created. If the contractor does not have access to NIWC Atlantic information system, the contractor shall send notice to the COR and [niwc\\_lant\\_mandtrn.fct@us.navy.mil](mailto:niwc_lant_mandtrn.fct@us.navy.mil). The following table is a sample of annual contractor mandatory training that is subject to change during the contract/order period of performance:

#	Training Course Name	Contractor Personnel Applicability
1	Controlled Unclassified Information (CUI)	All contractors
2	Records Management	All contractors NMCI account holders
3	Active Shooter, Level 1	All contractors
4	Sensitive Compartmented Information (SCI)	Contractors that are SCI cleared personnel and authorized users of DoD IS and networks
5	DoD Cyber Awareness Challenge	All contractors NMCI account holders and Personnel accessing CAC-enabled gov't sites – Authorized users of DoD information systems and networks
6	Privacy and Personally Identifiable Information (PII) Awareness Training	All contractors with access to PII
7	Suicide Prevention Training (Suicide Awareness)	All fulltime, onsite contractors
8	NIWC Atlantic Annual Security Refresher	All fulltime/partial, onsite contractors
9	NIWC Intelligence Oversight	All contractors
10	Operations Security (OPSEC)	All contractors
11	Antiterrorism Training, Level 1	Contractors requiring routine physical access to federally controlled facilities or

		military installations (DFARS 252.204-7004)
--	--	---

8.2.3.1 The contractor shall ensure applicable training is completed within the required due dates, or if employee onboards after the required due date, all applicable training is completed before the end of the fiscal year when the work is performed. The contractor shall ensure any additional and/or deleted training is verified with the COR. The contractor shall track and report all mandatory training required and completed for each employee in the Staffing Plan which is part of the monthly TOSR (CDRL A009). For CSWF, contractor shall ensure all mandatory cybersecurity training and certifications are reported in the CSWF Report (CDRL A008).

8.2.3.2 Contractor personnel shall utilize TWMS to complete all applicable mandatory training. If training is not applicable or contractor is unable to update TWMS, the contractor shall indicate status within the training section of the monthly status report. For some contractor personnel, attendance of Government face-to-face training is allowed if COR concurs with training schedule. For training taken via Defense Information Systems Agency/Navy Knowledge Online (DISA/NKO), the contractor shall forward a copy of the certificate to [niwc\\_lant\\_mandtrn.fct@us.navy.mil](mailto:niwc_lant_mandtrn.fct@us.navy.mil) who will upload or ensure each completed training is recorded in TWMS. The contractor shall report any training issues to the COR and the mandatory training functional email address.

8.2.3.3 The contractor shall educate employees on the procedures for the handling and production of classified material and documents, security clearance reporting requirements, and other security measures as described in the PWS in accordance with 32 CFR Part 117, NISPOM. The contractor shall ensure personnel complete any security-related training necessary to maintain proper access.

#### 8.2.4 Accessing Government Information Systems and Nonpublic Information

Contractor personnel shall meet the following cybersecurity and personnel security requirements when accessing Government information systems and nonpublic information.

Definition – For the purposes of this section, “sensitive information” includes the following:

- (a) all types and forms of confidential business information, including financial information relating to a contractor’s pricing, rates, or costs, and program information relating to current or estimated budgets or schedules.
- (b) source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC 2101-2107).
- (c) information properly marked as “business confidential,” “proprietary,” “procurement sensitive,” “source selection sensitive,” or other similar markings.
- (d) other information designated as sensitive by NIWC Atlantic and the program.

8.2.4.1 In the performance of the contract/order, the contractor may receive or have access to information, including information in Government Information Systems and secure websites. Accessed information may include “sensitive information” or other information not previously made available to the public that would be competitively useful on current or future related procurements.

8.2.4.2 Contractor personnel shall protect and safeguard from unauthorized disclosure all sensitive information to which they receive access in the performance of the contract/order, whether the information comes from the Government or from third parties. The contractor shall provide the following support:

- (a) Utilize accessed information and limit access to authorized users only for the purposes of performing the services as required by the contract/order, and not for any other purpose unless authorized.

(b) Safeguard accessed information from unauthorized use and disclosure, and not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the contract/order or as authorized by Federal statute, law, or regulation.

(c) Inform authorized users requiring access in the performance of the contract/order regarding their obligation to utilize information only for the purposes specified in the contract and to safeguard information from unauthorized use and disclosure.

(d) Execute a "Contractor Access to Information Non-Disclosure Agreement," and obtain and submit to the Contracting Officer a signed "Contractor Employee Access to Information Non-Disclosure Agreement" for each employee prior to assignment.

(e) Notify the Contracting Officer in writing of any violation of the requirements in Para 8.2.4.2(a) through Para 8.2.4.2(d) as soon as the violation is identified, no later than 24 hours. The notice shall include a description of the violation and the proposed actions to be taken, and shall include the business organization, other entity, or individual to whom the information was divulged.

8.2.4.3 In the event that the contractor inadvertently accesses or receives any information marked as "proprietary," "procurement sensitive," or "source selection sensitive," or that, even if not properly marked otherwise indicates the contractor may not be authorized to access such information, the contractor shall (i) Notify the Contracting Officer; and (ii) Refrain from any further access until authorized in writing by the Contracting Officer.

8.2.4.4 The requirements of this text are in addition to any existing or subsequent OCI requirements which may also be included in the contract/order, and are in addition to any personnel security or Cybersecurity/Information Assurance requirements, including SAAR form (DD Form 2875), annual Cybersecurity training certificate, federal background investigation questionnaire, or other forms that may be required for access to Government Information Systems.

8.2.4.5 Subcontracts. The contractor shall insert Para 8.2.4.1 through 8.2.4.4 in all subcontracts that may require access to sensitive information in the performance of the contract/order.

8.2.4.6 Mitigation Plan. If requested by the Contracting Officer, the contractor shall submit, within 45 calendar days following execution of the "Contractor Non-Disclosure Agreement," a mitigation plan (CDRL A00H) for Government approval, which shall be incorporated into the contract/order. At a minimum, the mitigation plan shall identify the contractor's plan to implement the requirements of Para 8.2.4.2 and shall include the use of a firewall to separate contractor personnel requiring access to information in the performance of the contract/order from other contractor personnel to ensure that the contractor does not obtain any unfair competitive advantage with respect to any future Government requirements due to unequal access to information. A "firewall" may consist of organizational and physical separation; facility and workspace access restrictions; information system access restrictions; and other data security measures identified, as appropriate. The contractor shall respond promptly to all inquiries regarding the mitigation plan. The contractor shall make necessary plan updates no later than 14 days after receipt of Government comments. Failure to resolve any outstanding issues or obtain approval of the mitigation plan within 45 calendar days of its submission may result, at a minimum, in rejection of the plan and removal of any system access.

#### 8.2.5 Handling of Personally Identifiable Information (PII)

In accordance with the Privacy Act of 1974, the contractor shall safeguard PII from theft, loss, and compromise. The contractor shall transmit and dispose of Personally Identifiable Information (PII) in accordance with the latest DoN policies. The contractor shall not store any Government PII on their

personal computers. The contractor shall mark all developed documentation containing PII information accordingly in the header and footer of each page of the document: "CUI". In addition to marking documents at the top and bottom with "CUI" a CUI "Designation Indicator Block" is required at the bottom of the document's first page within the "CUI" banner and footer markings. DoD guidance directs that this block be located at the lower right of the page. Any unauthorized disclosure of privacy sensitive information through negligence or misconduct can lead to contractor removal or contract termination depending on the severity of the disclosure. Upon discovery of a PII breach, the contractor shall immediately notify the Contracting Officer and COR. Once notified, the Contracting Officer shall immediately contact the Privacy Act Coordinator. Contractors responsible for the unauthorized disclosure of PII shall be held accountable for any costs associated with breach mitigation, including those incurred as a result of having to notify personnel. If a contractor, including any subcontractor, is authorized access to PII, the contractor shall complete annual PII training requirements and comply with all privacy protections under the Privacy Act.

### 8.3 OPERATIONS SECURITY (OPSEC) REQUIREMENTS

Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. OPSEC requirements are applicable when contract personnel have access to either classified information or unclassified Critical Program Information (CPI)/sensitive information. Pursuant to DoDD 5205.02E and SPAWARINST 3432.1, NIWC Atlantic's OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual and SPAWARSYSCENLANTINST 3070.1B.

#### 8.3.1 Local and Internal OPSEC Requirement

Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the NAVWAR-M-5510.1A and existing local site OPSEC procedures. The contractor shall develop their own internal OPSEC program specific to the task order and based on NIWC Atlantic OPSEC requirements. At a minimum, the contractor's program shall identify the current NIWC Atlantic site OPSEC Officer/Coordinator.

#### 8.3.2 OPSEC Training

The contractor shall track and ensure applicable personnel receive initial OPSEC training within 30 days of contract/task order award and annual OPSEC awareness training in accordance with requirements outlined in the Mandatory Training, Para 8.2.3. OPSEC training requirements are applicable for personnel during their entire term supporting this NIWC Atlantic task order.

#### 8.3.3 NIWC Atlantic OPSEC Program

The contractor shall participate in NIWC Atlantic OPSEC program briefings and working meetings, and the contractor shall complete any required OPSEC survey or data call within the timeframe specified.

#### 8.3.4 Classified Contracts

OPSEC requirements identified under a classified contract/order shall have specific OPSEC requirements listed on the DD Form 254.

### 8.4 INFORMATION SYSTEM SECURITY

Pursuant to DoDM 5200.01, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on task. The contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor,



information developed during the course of the task order, and privileged task order information (e.g., program schedules and task order-related tracking).

#### 8.4.1 Hardware and Software

The contractor shall scan all electronic deliverables or electronically provided information for malicious code using DoD approved anti-virus software prior to delivery to the Government. The contractor shall utilize appropriate controls (firewalls, password protection, encryption, digital certificates, etc.) at all times to protect task order related information processed, stored or transmitted on the contractor's and Government's computers/servers to ensure confidentiality, integrity, availability, authentication and non-repudiation. The contractor shall ensure Data-at-Rest encryption technology is installed on all portable electronic devices including storage of all types.

#### 8.4.2 Safeguards

The contractor shall protect Government information and shall be able to provide documentation (e.g., Systems Security Plan (SSP)) validating they are complying with the requirement in accordance with DFARS 252.204-7012. Subcontractors are subject to DFARS requirements only when performance will involve operationally critical support or covered defense information (CDI). The contractor shall not disclose any national defense information and shall safeguard procurement sensitive information, computer systems and data, Privacy Act regulations apply to all data, and DoD work products that are obtained or generated in the performance of this contract. This includes dissemination of protocols and papers not generally available through the public literature or websites. The contractor and all applicable subcontractors shall abide by the following safeguards:

8.4.2.1 Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.

8.4.2.2 Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

8.4.2.3 Sanitize media (e.g., overwrite, reformat, or degauss) before external release or disposal.

8.4.2.4 Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as portable hard drives and digital optical disks, using DoD Authorized Data-at-Rest encryption technology. Thumb drives are not authorized for DoD work, storage, or transfer. Use GSA Awarded DAR solutions (GSA # 10359) complying with ASD-NII/DOD-CIO Memorandum, "Encryption of Sensitive Unclassified Data-at-Rest on Mobile Computing Devices and Removable Storage." The contractor shall ensure all solutions meet FIPS 140-2 compliance requirements.

8.4.2.5 Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.

8.4.2.6 Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS). Encrypt organizational wireless connections and use encrypted wireless connection where available when traveling. If encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using at least application-provided password protection level encryption. The contractor shall encrypt or digitally sign all communications for authentication and non-repudiation.

8.4.2.7 Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.



8.4.2.8 Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).

8.4.2.9 Provide protection against computer network intrusions and data exfiltration, minimally including the following:

(a) Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.

(b) Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

(c) Prompt application of security-relevant software patches, service packs, and hot fixes.

8.4.2.10 As applicable, comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, critical program information (CPI), personally identifiable information, export controlled).

8.4.2.11 Immediately (not to exceed 24 hours of suspected incident recognition) report loss or unauthorized disclosure of information in accordance with contract/task order or agreement requirements and mechanisms to the COR. Suspected security infractions and incidents involve system equipment, electronic removeable media, malicious code, privileged user misuse, unauthorized user access, and/or suspected spillage of classified information to lower classification system.

8.4.2.12 Pursuant to DFARS 252.204-7009, the contractor shall not use or disclose third-party contractor reported cyber incident information. The contractor can be held liable for breach of information and shall extend restriction in subcontracts for service that include support to Government's activities related to safeguarding covered defense information and cyber incident reporting.

8.4.2.13 As applicable, follow minimum standard in SECNAVINST 5510.36B for classifying, safeguarding, transmitting, and destroying classified information and CUI.

8.4.2.14 Not disclose or cause the dissemination of information concerning operations of military activities that could result in violation of the contract and could result in legal actions. The contractor shall provide Registration Authority/Local Registration Authority (RA/LRA) services to the DoD and subcontractors. The contractor shall establish written procedures to ensure that any subcontractors on the contract are in compliance with the authoritative regulations as cited in this section, but not limited to.

#### 8.4.3 Compliance

Pursuant to DoDM 5200.01, the contractor shall include in their quality processes procedures that are compliant with information security requirements. In summary, the contractor shall be responsible for compliance with the latest cybersecurity DoD instructions, Risk Management Framework (RMF) guidance, orders, directives, and supplemental memorandums governing cybersecurity compliance with RA/LRA. The contractor personnel performing RA tasks set forth in this PWS will comply in accordance with the following latest authoritative regulations and sources:

- Committee on National Security Systems Instruction (CNSSI) 1300 – Instruction for NSS PKI X.509 Certificate Policy
- National Security Systems (NSS) Public Key Infrastructure (PKI) – Department of Defense (DoA) Registration Practice Statement (RPS)
- Department of Defense (DoD) Public Key Infrastructure (PKI) Registration Authority/Local Registration Authority (RA/LRA) – Certification Practice Statement (CPS)

#### 8.4.4 Covered Defense Information

The contractor shall identify all covered defense information, as defined in DFARS 252.204-7012, and apply markings when appropriate to all deliverables in accordance with DoDI 5200.48.

#### 8.4.5 Utilization of a Contractor Furnished Government-controlled Equipment

For the purposes of this contract/order, contractor-owned computer assets loaded with a secure Government furnished computing image loaded software will be known as Government Controlled Equipment (GCE). The contractor shall meet specific operational requirements when utilizing a Contractor furnished laptop with a Government-controlled software image (refer to section 9.0). At a minimum, contractor personnel shall comply with the following requirements when utilizing a Contractor issued Government-owned or Government-controlled computer:

8.4.5.1 Contractor personnel shall arrange with the appropriate Government personnel for contractor-owned computer assets to be loaded with appropriate Government software platform images.

8.4.5.2 All messages sent to/from utilize VPN connections.

8.4.5.3 All messages sent to/from are encrypted.

8.4.5.4 No storage of data on non-compliant networks (e.g., contractor's corporate systems).

8.4.5.5 Only government email (NMCI, mail.mil, etc.) is allowed to be used; absolutely NO Gmail, other personal systems, and NO corporate email that does not reside on NIST compliant systems shall be utilized.

8.4.5.6 All email must be sent between compliant systems – e.g., sending encrypted email to a private corporate account that resides on an uncompliant network, then decrypting and utilizing it is not allowed.

8.4.5.7 All stored information meets data-at-rest encryption standards – if using GFP, then use the same methods as networked devices (e.g., MS Bitlocker, Symantec Endpoint Security, etc.)

8.4.5.8 All data is housed on GFE shared storage location – ensures government can retrieve its data at any time.

8.4.5.9 In regard to processing, storing or transmitting CUI, no CUI is allowed on an information system not meeting configuration and security standards.

#### 8.4.6 Utilization of a mobile device

For the purposes of this requirement, a mobile/portable device includes, but not limited to, cellular phone, Blackberry, Personal Digital Assistant (PDA), iPad, and tablet Personal Computer (PC) that utilizes a mobile operating system (OS) (i.e., Apple iOS or Android). This requirement refers to all mobile devices including non-government-owned mobile devices (i.e., personal or company-provided).

8.4.6.1 CUI Protection – In accordance with DoD CIO memorandum of 10 Aug 22, "Use of Non-Government Owned Mobile Devices," the contractor shall ensure non-government-owned mobile device meets the "Approved Mobile Device (AMD)" criteria when it is used for storing, processing, transmitting, or displaying up to DoD CUI. The contractor shall not use non-DoD accounts or personal e-mail accounts, messaging systems or other non-public DoD information systems, except approved or authorized, to conduct official business involving CUI. The contractor shall not use unclassified systems, government-issued or otherwise, for classified national security information.

8.4.6.2 Electronic messaging – Electronic messaging includes online communications through websites, electronic mail (e-mail), texting, chat, and other related communications methods. Unless otherwise authorized by the government, non-official electronic messaging accounts must not be used to conduct official DoD communications in accordance with DoDI 8550.01. Pursuant to DoDI 5015.02, records created, sent, or received using electronic messaging accounts must be managed electronically, including the capability to identify, retrieve, and retain records for as long as they are needed, in accordance with part 1236.22 of Reference (c) and in accordance with National Archives and Records Administration (NARA) Bulletin 2012-02 or NARA Bulletin 2013-02, as applicable.

8.4.6.3 DoD Mobile Enterprise System – In accordance with DoD CIO memorandum of 27 Sep 23, "Use of Text Messaging on Mobile Devices and Records Management of Electronic Messages," the contractor conducting government business utilizing a government-owned mobile device or a non-government owned mobile device shall use Microsoft Teams Chat for text messaging as the designated fully managed DoD Mobile Enterprise System. Records created or received in Microsoft Teams Chat will be managed within the application and no additional copy of the record will be required. When mission needs or the effective conduct of DoD business cannot be adequately supported by Microsoft Teams Chat, SMS texting may be used in accordance with DoDI 8170.01. In such cases, the contractor shall forward a complete copy of the record to an official DoD electronic messaging account of the user within 20 days of the record's original creation or transmission in accordance with Section 2911 of Title 44 U.S.C. and Component processes. The complete copy of the record includes the content of the message and required metadata. The contractor shall be able to retrieve the record which must be usable in compliance with the applicable retention schedule approved by the Archivist of the United States.

## 8.5 ENHANCED SECURITY CONTROLS

The contractor shall not process, store, or transmit controlled unclassified information (CUI), as defined in DoDI 5200.48, on any information system and IT asset that is owned, or operated by or for, the contractor except for computer assets identified as Government controlled equipment (GCE).

## 9.0 GOVERNMENT FURNISHED INFORMATION (GFI)

For the purposes of this task order, Government Furnished Information (GFI) includes manuals, technical specifications, software, software licenses, maps, building designs, schedules, drawings, test data, etc. provided to contractors for performance on this task order. Depending on information contained in a document, the contractor shall comply with additional controls (e.g., completion of a Non-Disclosure Agreements, etc.) for access and distribution. The Government will mark any CUI which includes unclassified covered defense information and unclassified controlled technical information provided to the contractor. For any missing markings, contractor shall request appropriate marking from the Government.

GFI is utilized on this task order. Any applicable document (PWS Para 16.0) not available online, the Government will provide document as GFI listed in the table below. The contractor shall inventory all GFI by tracking distribution and location and provide a GFI inventory to the Government. The contractor shall use the GFI provided to support this task order only – use of GFI document(s) to

support other projects beyond this task order is not allowed. Unless otherwise specified, all GFI will be provided by the Government by the estimated delivery date listed in the table below, and the contractor shall return all GFI to the Government at completion of the task order. If a contractor requires additional GFI other than what is listed, the contractor shall submit a request to the COR within 30 days after task order award.

Item #	Description	GFI Estimated Delivery Date
1	Microsoft Windows computing platform image	14 days after task order award

## 10.0 GOVERNMENT PROPERTY

As defined in FAR Part 45, Government property is property owned or leased by the Government which includes Government-furnished property (GFP) and Contractor-acquired property (CAP). Government property is material, equipment, special tooling, special test equipment, and real property.

The contractor shall have established property management procedures and an appropriate property management point of contact who shall work with the assigned Government Property Administrator to ensure their property management system is acceptable. Government property does not include intellectual property and software.

### 10.1 GOVERNMENT-FURNISHED PROPERTY (GFP)

As defined in FAR Part 45, GFP is property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract/order. GFP includes spares and property furnished for repair, maintenance, overhaul, or modification. GFP includes Government-furnished equipment (GFE), Government-furnished material (GFM), Special Tooling (ST) and Special Test Equipment (STE).

GFP will not be provided on this task order.

### 10.2 CONTRACTOR-ACQUIRED PROPERTY (CAP)

As defined in FAR Part 45, CAP is property acquired, fabricated, or otherwise provided by the contractor for performing a contract and to which the Government has title but has not yet performed receipt and acceptance. CAP consists of Contractor-acquired equipment (CAE), Contractor-acquired material (CAM), ST, and STE.

CAP may be wholly provided to NIWC Atlantic, incorporated into a system, consumed, or delivered as an end item in the performance of the task order. Pursuant to SPAWARINST 4440.12A, the contractor shall provide CAP identified in the following table.

Prior to CAP items being acquired, fabricated, or otherwise provided, the contractor shall obtain COR concurrence. Exact items and quantities of equipment and material are subject to change after task order award. The identified CAP items are an estimate of various associated cost based on historical data.

Item #	Description, CAP	Part #	Unit/Issue	Quantity	IAW PGI 245.402-71, item to be delivered under a line item? (Y/N)
1	Miscellaneous Computer Peripherals	Various	Lot	1	N

2	Miscellaneous Cables	Various	Lot	1	N
3	Miscellaneous Communication Devices	Various	Lot	1	N

### 10.3 GOVERNMENT PROPERTY MANAGEMENT

#### 10.3.1 Designated Government Property Administrator

Pursuant to FAR Subpart 42.201, the task order Government Property Administrator (PA) is the assigned Administration Office unless otherwise designated. The contractor shall work with the Contracting Officer appointed PA to ensure compliance with the contract's property requirements in accordance with DoDI 4161.02 and the Guidebook for Contract Property Administration.

#### 10.3.2 Contractor Property Management System

Pursuant to DFARS 252.245-7003, the contractor shall establish and maintain an acceptable property management system that is subject to review and approval by the Contracting Officer and contract/order PA. The contractor's property management system shall adhere to the applicable prescribed requirements in FAR 52.245-1. The contractor shall be capable of reviewing property according to type property (i.e., GFP, CAP, or NMCI). For contractors without an approved property management system, the contractor shall contact the appointed PA within 30 days of task order award and provide a copy of their property management procedures with the names of appropriate point(s) of contact.

#### 10.3.3 Government Property Tracking and Reporting

The contractor shall track, maintain, and report all Government property accountable to the contract/order. All contractor personnel shall be responsible for following the company's internal inventory management procedures and correcting any problems noted by the Government PA. The contractor shall ensure property records maintain within property management system are complete, current, and auditable for all GP transactions. The contractor shall ensure GP records contain, at a minimum, the data elements as described in FAR 52.245-1 and if applicable data elements specified in the DFARS 252.245-7005. The contractor shall address any GP concerns and problems (e.g., receipt delays, tracking issues, etc.) in the monthly TOSR (CDRL A009).

10.3.3.1 CAP – The contractor shall provide a CAP inventory list as part of the monthly TOSR (CDRL A009). The contractor shall report each item purchased or fabricated, date of receipt if applicable, and the disposition of each item within the reporting period. For items to be delivered to the Government and not consumed or integrated into equipment or system, the contractor shall provide the required data items as specified under the CAP delivery requirements.

#### 10.3.4 Government Property Record/Pass

Pursuant to FAR 52.245-1, contractors and any subcontractors if applicable shall be responsible for establishing and maintaining records of Government Property in their possession.

#### 10.3.5 Government Property Transferring Accountability

Unlike GFP, CAP cannot be transferred. If CAP is required to be utilized on a contract/task order other than the one that funded its acquisition, the contractor shall deliver all CAP items to the Government. Once received and accepted by the Government, the previously known CAP items will be provided to the contractor as GFP on the same or different contract.

#### 10.3.6 Government Property Lost or Damaged Items

The contractor shall promptly report to the COR and Contracting Officer all lost and/or damaged Government property. Pursuant to DFARS 252.245-7005, the contractor shall report loss in the GFP module. In accordance with FAR 52.245-1 and the applicable DFARS clause, the contractor shall have internal processes established to report, respond, and mitigate loss of Government Property. If

the contractor disposes of any GP without proper authorization, the GP is considered lost, and the contractor shall manage item(s) as property loss.

#### **10.3.7 Government Property Delivery and Disposition**

The contractor shall document the delivery of any GP which can occur anytime during the life of the contract/order. As part of the Closeout Report (CDRL A00D), the contractor shall submit a comprehensive GP Closeout list. Disposition instructions for some GP may be contained in the accountable contract or on the supporting shipping documents (DD Form 1149). In the submitted closeout list, the contractor shall specify status of all applicable GP items (i.e., consumed, excess, installed/integrated, destroyed, missing, delivered to NIWC Atlantic, reutilized, transferred, or awaiting disposition instructions). The contractor shall submit the list to the COR and Contracting Officer, via the activity PA, at which time disposition instructions will be provided by the Government. For GP intended for demilitarization, mutilation, or destruction by the contractor, the event shall be witnessed and verified by the COR or designated Government personnel. The COR is ultimately responsible for directing disposition which includes sending items to Defense Reutilization and Marketing Office (DRMO). If required, the contractor shall include a follow-up GP Closeout list outlining final disposition as a supplement to the Closeout Report.

**10.3.7.1 CAP** – The contractor shall deliver all CAP items not consumed or integrated to the Government unless the Government has directed otherwise. Any delivered uniquely identifiable CAP item as outlined in PGI 245.402-71, will be accepted by the Government on a not-separately-priced (NSP) line item (CLIN/SLIN/ELIN) which can be established at time of contract/order award or post award. For CAP items requiring a NSP line item to be created post award, the contractor shall provide the following data items as part of the monthly status report:

- (i) Line item number
- (ii) Item description
- (iii) Either an NSN, Part Number and CAGE, or Model Number
- (iv) Quantity
- (v) Unit of Measure
- (vi) Date Placed in service by the contractor

At the completion of the contract/order, the contractor shall coordinate with the Government concerning all remaining item dispositioned (which includes all deliverable items and all unused/non-consumed material items). The contractor shall note final status of all CAP items in the GP inventory list.

#### **10.3.8 Government Property Performance Evaluation**

Non-compliance with Government Property terms and conditions will negatively affect the contractor's annual CPARS rating.

### **10.4 TRANSPORTATION OF EQUIPMENT/MATERIAL**

Transportation of equipment/material is not required by the contractor on this task order.

## **11.0 TRAVEL**

### **11.1 LOCATIONS**

The contractor shall, at a minimum, be prepared to travel to the locations listed within this section. Travel outside of the contiguous United States (OCONUS) is required. Exact travel dates and locations are subject to change. Prior to travel, the contractor shall meet all necessary travel requirements for their company and personnel to perform work in the noted locations including all foreign OCONUS sites. Contractor personnel traveling in support of DoD shall travel in accordance with the latest Joint Travel Regulations (JTR) at time travel is being performed. The contractor shall comply with travel

cost pursuant to FAR 31.205-46. The contractor shall notify the COR prior to traveling to ensure Government coordination and approval.

**BASE THRU OY4, IF EXERCISED**

<b># Trips</b>	<b># People</b>	<b># Days/Nights</b>	<b>From (Location)</b>	<b>To (Location)</b>
8	5	5, 4	Charleston, SC	Bethesda, MD
4	2	6, 5	Charleston, SC	Guantanamo Bay
4	2	14, 13	Charleston, SC	Yokosuka, Japan
4	2	5, 4	Charleston, SC	Corpus Christi, TX
4	2	5, 4	Charleston, SC	Portsmouth, VA
6	2	14, 13	Charleston, SC	Rota, Spain
2	2	5, 4	Charleston, SC	Fort Hood, TX
2	2	5, 4	Charleston, SC	Fort Irwin, CA
2	2	5, 4	Charleston, SC	Aberdeen, MD
2	2	5, 4	Charleston, SC	Fort Meade, MD
2	2	5, 4	Charleston, SC	Fort Jackson, SC
2	2	5, 4	Charleston, SC	Fort Drum, NY
2	2	5, 4	Charleston, SC	Fort Lee, VA
2	2	5, 4	Charleston, SC	Fort Knox, KY
2	2	5, 4	Charleston, SC	Carlisle Barracks, PA
3	4	10, 9	Charleston, SC	Honolulu, HI
2	2	5, 4	Charleston, SC	Fort Rucker, AL
2	2	5, 4	Charleston, SC	Fort Riley, KS
4	2	5, 4	Charleston, SC	Fort Belvoir, VA
2	2	5, 4	Charleston, SC	West Point, NY
2	2	5, 4	Charleston, SC	Fort Eustis, VA
2	5	14, 13	Charleston, SC	San Francisco, CA
4	2	5, 4	Charleston, SC	Dulles, VA
4	4	10, 9	Charleston, SC	NH Beaufort
6	5	5, 4	Charleston, SC	Bremerton, WA
2	6	5, 4	Charleston, SC	San Diego, CA
2	6	5, 4	Charleston, SC	Jacksonville, NC
4	4	14, 13	Charleston, SC	Stuttgart, Germany
3	2	14, 13	Charleston, SC	Naples, Italy
2	2	14, 13	Charleston, SC	Sicily, Italy
2	2	14, 13	Charleston, SC	Jakarta, Indonesia
2	4	5, 4	Charleston, SC	Biloxi, MS
2	2	5, 4	Charleston, SC	Dayton, OH
2	4	6, 5	Charleston, SC	Spokane, WA
4	2	4, 3	Charleston, SC	Norfolk, VA
2	2	5, 4	Charleston, SC	Washington, DC
2	2	14, 13	Charleston, SC	Seoul, South Korea
2	1	5, 4	Honolulu, Hawaii	Charleston, SC
2	1	14, 13	Stuttgart, Germany	Charleston, SC

**OY5, IF EXERCISED**

<b># Trips</b>	<b># People</b>	<b># Days/Nights</b>	<b>From (Location)</b>	<b>To (Location)</b>
4	5	5, 4	Charleston, SC	Bethesda, MD
2	2	6, 5	Charleston, SC	Guantanamo Bay

2	2	14, 13	Charleston, SC	Yokosuka, Japan
2	2	5, 4	Charleston, SC	Corpus Christi, TX
2	2	5, 4	Charleston, SC	Portsmouth, VA
3	2	14, 13	Charleston, SC	Rota, Spain
1	2	5, 4	Charleston, SC	Fort Hood, TX
1	2	5, 4	Charleston, SC	Fort Irwin, CA
1	2	5, 4	Charleston, SC	Aberdeen, MD
1	2	5, 4	Charleston, SC	Fort Meade, MD
1	2	5, 4	Charleston, SC	Fort Jackson, SC
1	2	5, 4	Charleston, SC	Fort Drum, NY
1	2	5, 4	Charleston, SC	Fort Lee, VA
1	2	5, 4	Charleston, SC	Fort Knox, KY
1	2	5, 4	Charleston, SC	Carlisle Barracks, PA
2	4	10, 9	Charleston, SC	Honolulu, HI
1	2	5, 4	Charleston, SC	Fort Rucker, AL
1	2	5, 4	Charleston, SC	Fort Riley, KS
2	2	5, 4	Charleston, SC	Fort Belvoir, VA
1	2	5, 4	Charleston, SC	West Point, NY
1	2	5, 4	Charleston, SC	Fort Eustis, VA
1	5	14, 13	Charleston, SC	San Francisco, CA
2	2	5, 4	Charleston, SC	Dulles, VA
2	4	10, 9	Charleston, SC	NH Beaufort
3	5	5, 4	Charleston, SC	Bremerton, WA
1	6	5, 4	Charleston, SC	San Diego, CA
1	6	5, 4	Charleston, SC	Jacksonville, NC
2	4	14, 13	Charleston, SC	Stuttgart, Germany
2	2	14, 13	Charleston, SC	Naples, Italy
1	2	14, 13	Charleston, SC	Sicily, Italy
1	2	14, 13	Charleston, SC	Jakarta, Indonesia
1	4	5, 4	Charleston, SC	Biloxi, MS
1	2	5, 4	Charleston, SC	Dayton, OH
1	4	6, 5	Charleston, SC	Spokane, WA
2	2	4, 3	Charleston, SC	Norfolk, VA
1	2	5, 4	Charleston, SC	Washington, DC
1	2	14, 13	Charleston, SC	Seoul, South Korea
2	1	5, 4	Honolulu, Hawaii	Charleston, SC
2	1	14, 13	Stuttgart, Germany	Charleston, SC

## 11.2 OCONUS TRAVEL REQUIREMENTS

OCONUS travel includes travel outside of the Contiguous United States (CONUS) as define in FAR 2.101. Pursuant to SPAWARSYSCENLANTINST 12910.1B, DoDD 4500.54E, and the latest DoD Foreign Clearance Guide (FCG) requirements, the contractor shall travel to OCONUS sites to support deployed forces. The contractor shall be familiar with and able to obtain approvals in the Aircraft and Personnel Automated Clearance System (APACS) as well as submitting and requesting letter of authorization (LOA) in the web-based Synchronized Pre-deployment & Operational Tracker (SPOT).

### 11.2.1 General OCONUS Requirements

The contractor shall ensure compliance with applicable clauses and travel guide requirements (including completion of any mandatory training) prior to traveling to each of the specified travel



locations. The contractor shall be responsible for knowing and understanding all travel requirements as identified by the applicable combatant command (CCMD) and country. For all OCONUS travel, the contractor shall submit an official OCONUS Travel Request for each person traveling via the Generic Approval App Builder (GAAB) / Scalable Workforce Automation Tool (SWAT) program. The contractor shall access the module: Travel - Official OCONUS – CTR and ensure all OCONUS travel has APACS approval. The travel request and any necessary forms are required to be completed and uploaded no later than 30 days prior to travel – shorter time frame may be necessary to accommodate time sensitive support. The contractor shall ensure personnel traveling OCONUS has current contact information entered in Navy Family Accountability and Assessment System (NFAAS) prior to traveling.

#### **11.2.2 OCONUS Immunization Requirements**

Pursuant to DoDI 6205.4, SPAWARSYSCENLANTINST 12910.1B, and any additional DON specific requirements, contractor employees who deploy to OCONUS locations both shore and afloat shall require up to date immunizations. The contractor shall review and verify if their personnel meet any immunization requirements prior to assigning personnel to travel.

#### **11.2.3 Emergency Medical Screening for OCONUS Travel**

During emergency related situations including health (e.g., COVID-19 pandemic) and weather-related circumstances, contractor personnel shall perform official OCONUS travel in accordance with the latest directions outlined in the NIWC Atlantic COG, related DoD travel websites, and the Centers for Disease Control and Prevention (CDC) website. To the extent possible, contractor personnel shall follow the same travel regulations and restrictions as Government civilian personnel. When in doubt concerning applicability, the contractor shall verify requirements with COR and NIWC Atlantic OCONUS Travel Team. Depending on the latest travel regulations which may differ based on location, contractor personnel shall be prepared to meet additional requirements such as medical testing prior to travel. These requirements will be identified by the COR. Contractor personnel shall complete any required health screening/testing and complete screening questionnaire which shall all be submitted to the COR prior to travel.

#### **11.2.4 Letter of Authorization**

The contractor shall have a LOA signed by the designated Contracting Officer for any and all OCONUS Travel. An OCONUS Travel Form for contractors (NIWCLANT 12990/12, Rev 06/21) is required for all travel locations OCONUS to include Alaska, Guam, Hawaii, Kwajalein Atoll, Johnston Atoll, Midway Islands/Atoll, Puerto Rico, US Virgin Islands, Wake Island, etc. If the travel location is not in "the lower 48"/CONUS, then an OCONUS Travel Form is required prior to the LOA being Government Authorized by an employee of the NIWC Atlantic OCONUS Travel Team in order for the Contracting Officer to approve. The LOA identifies any additional authorizations, privileges, or Government support that contractor personnel are entitled to under contract and task order, if applicable. The contractor shall initiate a LOA for each prospective traveler. The contractor shall use SPOT or its successor, at <https://spot.dmdc.mil/privacy.aspx>, to enter and maintain data with respect to traveling/deployed personnel, and to generate LOAs. When necessary and if in the Government's interest, the contractor may also initiate a LOA request to provide an official traveler access to Government facilities and to take advantage of travel discount rates in accordance with Government contracts and/or agreements. All privileges, services, and travel rate discount access are subject to availability and vendor acceptance. LOAs are required to be signed and approved by the SPOT registered Contracting Officer of this task order. Contractor personnel traveling in support of NIWC Atlantic shall travel with a hardcopy approved LOA in their possession.

## **12.0 SAFETY ISSUES**

### **12.1 OCCUPATIONAL SAFETY AND HEALTH REQUIREMENTS**

The contractor shall be responsible for ensuring the safety of all company employees, other working personnel, and Government property. The contractor is solely responsible for compliance with the Occupational Safety and Health Act (OSHA) (Public Law 91-596) and the resulting applicable standards, OSHA Standard 29 CFR 1910 (general), 1915 (shipboard/submarine) and 1926 (shore), and for the protection, safety and health of their employees and any subcontractors assigned to the task orders. Without Government assistance, the contractor shall make certain that all safety requirements are met, safety equipment is provided, and safety procedures are documented as part of their quality management system. If performing within Government facilities, contractor shall immediately report any accidents involving Government or contractor personnel injuries or property/equipment damage to the Contracting Officer and COR. Additionally, the contractor is responsible for securing the scene and impounding evidence/wreckage until released by the COR or on-site Government representative.

### **13.0 SUBCONTRACTING REQUIREMENTS**

If the prime contractor is planning to utilize subcontractor(s) on this task order, the prime contractor shall identify the applicable subcontractor(s) in its proposal for the task order. Should the prime contractor be awarded a task order, only those subcontractors included in the proposal upon which the award is based are approved for use on the task order. Post award subcontractor additions (i.e. subcontractor additions to a task order after issuance of the order) are governed by FAR 52.244-2.

In addition, while Government consent to subcontract is not required for prime contractors with an approved purchasing system, if after award of a task order the prime contractor intends to enter into a subcontract with an entity not identified in its proposal upon which the task order award was based, the prime contractor shall nevertheless notify the Contracting Officer reasonably in advance of entering into any (i) cost-plus-fixed-fee subcontract, or (ii) fixed-price subcontract that exceeds either the simplified acquisition threshold or 5 percent of the total estimated cost of the task order. Such notification shall include, (i) a description of the supplies or services to be subcontracted, (ii) identification of the subcontract type to be used, (iii) identification of the proposed subcontractor, and (iv) the proposed subcontract price.

#### **13.1 AUTHORIZED SUBCONTRACTORS**

The following subcontractor(s) is either identified by the contractor at the time of award of the task order, have been consented to by the Government pursuant to the Subcontracts clause of the contract, or, in the event the contractor has an approved purchasing system, the contractor has provided notification in accordance with paragraph 13.0 above: ***[If applicable, contract specialist will list authorized subcontractors identified at time of award.] Contract Specialist to list authorized subcontractor(s); if no subcontractor(s) is applicable, Contract Specialist should enter “No subcontractor(s) identified.”***

### **14.0 ACCEPTANCE PLAN**

Inspection and acceptance is performed by the COR on all services, data, and non-data deliverables in accordance with the QASP, Attachment #1.

### **15.0 OTHER CONDITIONS/REQUIREMENTS**

#### **15.1 EXTENDED WORK WEEK**

Due to operational requirements, schedules, and the availability of required resources and/or downtime of those resources, extended work week (EWW) may be required for professional (i.e., salaried) employees. Prior to EWW hours worked, the contractor shall obtain COR concurrence for the specific hours per labor category and applicable dates.

## 15.2 WORKWEEK

All or a portion of the effort under this task order will be performed on a Government installation. The contractor shall provide support services corresponding to Government workweek and core hours. Normal workweek is Monday through Friday. Normal business hours occur 0730-1600 local standard time (LST) based on location of work. Pursuant to Federal law (5 U.S.C. 6103), the Government observes the following public holidays per year. For planning purposes, contractors working in Government spaces shall treat these holidays as Government non-workdays which may affect accessibility to Government space.

<u>Name of Holiday</u>	<u>Time of Observance</u>
New Year's Day	1 January
Martin Luther King Jr. Day	Third Monday in January
President's Day	Third Monday in February
Memorial Day	Last Monday in May
Juneteenth	19 June
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veteran's Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

If any of the above holidays occur on a Saturday or a Sunday, then such holiday will be observed by the Government on the prior Friday or following Monday, respectively.

## 15.3 OVERTIME FOR SCLS LABOR CATEGORIES

Work will be performed during normal working hours when practical. Due to operational requirements, schedules, and the availability of required resources and/or downtime of those resources, overtime (OT) will be allowed for Service Contract Labor Standards (SCLS) labor categories in accordance with FAR 52.222-2. This task order does not allow for payment of overtime during the normal workweek for employees who are exempt from the Fair Labor Standards Act unless expressly authorized by the Contracting Officer. Under Federal regulations, the payment of overtime is required only when a non-exempt employee works more than 40 hours in a normal week period. Prior to working OT hours, the contractor shall obtain COR concurrence for the specific hours per labor category and applicable dates.

## 15.4 NON-DISCLOSURE AGREEMENT (NDA) REQUIREMENTS

All contractor personnel who receive or have access to proprietary information shall sign and abide by a non-disclosure agreement (Attachment #4).

## 15.5 TRANSITIONAL PLAN

To minimize loss in productivity and to mitigate negative impact to on-going support services when new contractors are introduced, the contractor shall provide support during the transition-in and transition-out periods. The contractor shall have personnel on board within the first sixty days after award. Note: this time period is part of funded contract/TO transitional periods at the beginning and end of the contract/task order. After contract/ task order award (transition-in), the contractor shall work with the exiting contractor and become familiar with performance requirements in order to commence full performance of services before the out-going contractor leaves the site. Prior to the

completion of the contract/ task order (transition-out), the contractor shall work with any new contractor personnel to ensure continuous support between contracts.

#### 15.6 RELOCATION

This task order will provide the following relocation reimbursement expenses in support of regional network security operations:

		Base Period	Option Period 1	Option Period 2	Option Period 3	Option Period 4	Option Period 5
Description	Unit/Issue	Quantity					
Relocation/Repatriation	Per person	1	1	1	1	1	1
DoD Schools	Per person	3	3	3	3	3	3
Living Quarters Allowance	Per person	1	1	1	1	1	1
Defense Base Act Insurance	Per person	1	1	1	1	1	1

#### 15.7 ACCESS TO CLASSIFIED NETWORKS

The contractor will require access to classified government computers/networks to include NIPR, SIPR, other classified SCI networks and systems relevant to task order's scope of work, as well as NSAnet.

### 16.0 APPLICABLE DOCUMENTS (AND DEFINITIONS)

The contractor shall ensure all work accomplished utilizes the latest, relevant industry practices and standards when applicable unless otherwise indicated by text. In accordance with Defense Acquisition Policy, maximum utilization of non-Government standards will be made wherever practical.

#### 16.1 REQUIRED DOCUMENTS

The contractor shall utilize the following mandatory documents in support of this task order. The documents referenced in this section list the minimum version dates; however, the contractor shall meet requirements for any referenced document including subsequent updates applicable at time the task order request for proposal is posted.

	Document Number	Title
a.	DoNM 1000.13-M-V1	DoD Manual – DoD Identification (ID) Cards: ID Card Life-Cycle, Volume 1 dtd 23 Jan 14 with Change 1 dtd 28 Jul 20
b.	DoDI 5015.02	DoD Instruction – DoD Records Management Program dtd 24 Feb 15 with Change 1 dtd 17 Aug 17
c.	DoDM 5200.01	DoD Manual – Information Security Program (vol 1, 2, 3 ) dtd 24 Feb 12 with Change 2/4/3 dtd 28 Jul 20
d.	DoDD 5205.02E	DoD Directive – Operations Security (OPSEC) Program dtd 20 Jun 12 with Change 2 dtd 20 Aug 20
e.	DoDM 5205.02	DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08 with Change 1 dtd 26 Apr 18
f.	DoDI 5200.46	DoD Instruction – DoD Investigation and Adjudicative Guidance for issuing the Common Access Card (CAC) dtd 9 Sep 14 with Change 2 dtd 2 Nov 20

	<b>Document Number</b>	<b>Title</b>
g.	DoDI 5200.48	DoD Instruction – Controlled Unclassified Information (CUI) dtd 6 Mar 20
h.	DoDI 5230.24	DoD Instruction – Distribution Statements on Technical Information dtd 10 Jan 23
i.	DoDI 6205.4	DoD Instruction – Immunization of Other Than U.S. Forces (OTUSF) for Biological Warfare Defense dtd 14 Apr 00
j.	DoDD 8140.01	DoD Directive – Cyberspace Workforce Management dtd 05 Oct 20
k.	DoDM 8140.03	DoD Manual - CYBERSPACE WORKFORCE QUALIFICATION AND MANAGEMENT PROGRAM
l.	DoDI 8170.01	DoD Instruction – Online Information Management and Electronic Messaging, Change 1 dtd 24 Aug 21
m.	DoDI 8500.01	DoD Instruction – Cybersecurity dtd 14 Mar 14 with Change 1 dtd 07 Oct 19
n.	DoDI 8510.01	DoD Instruction – Risk Management Framework (RMF) for DoD Information Technology (IT) dtd 12 Mar 14 with Change 2 dtd 28 Jul 17
o.	DoDI 8550.01	DoD Instruction – DoD Internet Services and Internet-Based Capabilities dtd 11 Sep 12
p.	DON CIO Memorandum	Acceptable Use of Department of the Navy Information Technology (IT) dtd 25 Feb 20
q.	SECNAV M-5239.2	Secretary of the Navy Manual – DON Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual dtd June 2016 (and subsequent revisions)
r.	SECNAVINST 5239.3C	Secretary of the Navy Instruction – DoN Cybersecurity Policy dtd 2 May 16
s.	SECNAVINST 5239.20A	Secretary of the Navy Instruction – DoN Cyberspace IT and Cybersecurity Workforce Management and Qualification dtd 10 Feb 16
t.	SECNAVINST 5510.30C	Secretary of the Navy Instruction – DoN Personnel Security Program (PSP) Instruction dtd 6 Oct 06
u.	SECNAVINST 5510.36B	Secretary of the Navy Instruction – DoN Information Security Program dtd 12 Jul 19
v.	SPAWARSCENLANT INST 3070.1B	Space and Naval Warfare Systems Center Atlantic Instruction – Operations Security Policy dtd 20 Jan 17
w.	SPAWARSCENLANT INST 12910.1B	Space and Naval Warfare Systems Center Atlantic Instruction – Deployment of Government and Contractor Personnel Outside the Continental United States dtd 23 Aug 16
x.	NAVWAR M-5510.1A	Naval Information Warfare Systems Command Security Manual, dtd Nov 21
y.	Navy Telecommunications Directive (NTD 10-11)	System Authorization Access Request (SAAR), DD Form 2875, May 2022 revision
z.	JTR	The Joint Travel Regulations (JTR) – Uniformed Service Members and DoD Civilian Employees
aa.	32 CFR Part 117 NISPOM	32 Code of Federal Regulation Part 117 – National Industrial Security Program Operating Manual (NISPOM) dtd 24 Aug 21

	Document Number	Title
ab.	Section 508 of the Rehabilitation Act of 1973	United States federal law, as amended, 29 U.S.C. § 794d
ac.	Privacy Act of 1974	United States federal law, Pub.L. 93–579, 88 Stat. 1896, dtd December 31, 1974, 5 U.S.C. § 552a
ad.	CNSSI-1300	Committee on National Security Systems Instruction (CNSSI) 1300, version 2, dtd December 2021, Instruction for Secret National Security Systems Public Key Infrastructure X.509 Certificate Policy
ae.	NSS PKI DoD RPS	National Security System (NSS) Public Key Infrastructure (PKI) Department of Defense (DoD) Registration Practice Statement (RPS), version 14, dtd 13 July 2022 and all subsequent versions
af.	DoD PKI RA/LRA CPS	Department of War (DoD) Public Key Infrastructure (PKI) Registration Authority/Local Registration Authority (RA/LRA) Certification Practice Statement (CPS), version 8, dtd 13 July 2022 and all subsequent versions

## 16.2 GUIDANCE DOCUMENTS

The contractor shall utilize the following guidance documents in support of this task order. The documents referenced in this section list the minimum version dates; however, the document's effective date of issue is the task order's request for proposal issue date.

	Document Number	Title
a.	MIL-STD-130N	DoD Standard Practice – Identification Marking of US Military Property
b.	MIL-STD-1916	DoD Test Method Standard – DoD Preferred Methods for Acceptance Of Product
c.	DoDM 1000.13-M-V1	DoD Manual – DoD Identification Cards: ID card Life-Cycle, Volume 1, dtd 23 Jan 14
d.	DoDD 4500.54E	DoD Directive – DoD Foreign Clearance Program (FCP) w/ Change 1 dtd 24 May 17
e.	DoDD 5000.01	DoD Directive – The Defense Acquisition System dtd 20 Nov 07
f.	DoDI 5000.02	DoD Instruction – Operation of the Defense Acquisition System dtd 7 Jan 15
g.	HSPD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors dtd 27 Aug 04
h.	FIPS PUB 201-3	Federal Information Processing Standards Publication 201-2 – Personal Identity Verification (PIV) of Federal Employees and Contractors, January 2022
i.	Form I-9, OMB No. 1615-0047	US Department of Justice, Immigration and Naturalization Services, Form I-9, OMB No. 1615-0047 – Employment Eligibility Verification
j.	N/A	DoD Foreign Clearance Guide – <a href="https://www.fcg.pentagon.mil/fcg.cfm">https://www.fcg.pentagon.mil/fcg.cfm</a>

## 16.3 SOURCE OF DOCUMENTS

The contractor shall obtain all applicable documents necessary for performance on this task order. Many documents are available from online sources. Specifications and commercial/industrial documents may be obtained from the following sources:

Copies of Federal Specifications may be obtained from General Services Administration Offices in Washington, DC, Seattle, San Francisco, Denver, Kansas City, MO., Chicago, Atlanta, New York, Boston, Dallas and Los Angeles.

Copies of military specifications may be obtained from the Commanding Officer, Naval Supply Depot, 3801 Tabor Avenue, Philadelphia, PA 19120-5099. Application for copies of other Military Documents should be addressed to Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Ave., Philadelphia, PA 19120-5099.

All other commercial and industrial documents can be obtained through the respective organization's website.

***THE FOLLOWING LIST AND QUESTION BELOW IS NOT PART OF THE FINAL PWS – IT IS TO BE USED FOR PR PACKAGE REVIEW & 2.0 VALIDATION ONLY; Tech Code/IPT do not delete the following from PWS; Contract Specialist is responsible for deleting prior to incorporation into contract writing system:***

*(Tech Code should indicate if attachments is provided as part of PR package.)*

**LIST OF EXHIBITS & ATTACHMENTS**

- ☐ **Provided** Exhibit A -- CDRLs - DD FORM 1423
- ☒ **Provided** Attachment 1 – Quality Assurance Surveillance Plan (QASP)
- ☐ **Provided** Attachment # -- Consolidated GFP Form
- ☐ **Provided** Attachment # -- Contractor Acquired Property (CAP)
- ☐ **Provided** Attachment # -- Warranty Tracking Information (WTI) form
- ☐ **Provided** Attachment # -- Source of Repair Instructions (SORI) form
- ☐ **Provided** Attachment 2 -- Specific Location Requirements
- ☐ **Provided** Attachment 3 – Hardware APL Guidance
- ☐ **Provided** Attachment # -- Estimated Travel Requirements
- ☐ **Provided** Attachment # -- Alternative Travel Locations
- ☒ **Provided** Attachment 4 -- Non-Disclosure Agreement (NDA) form
- ☐ **Provided** Attachment # -- Theater Business Clearance (TBC) Clauses/Instructions (Dec 2020)