# PERFORMANCE WORK STATEMENT (PWS)

## Defense Technology Security Administration
## Application Management Services
## September 7, 2022

### Part 1

### General Information

## 1. GENERAL

This is a non-personal services contract to provide Application Management Services (AMS) for the Defense Technology Security Administration (DTSA). The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn is responsible to the Government.

### 1.1. Description of Services/Introduction

The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to Application Management Services as defined in this Performance Work Statement except for those items specified as government furnished property and services. The contractor shall perform to the standards in this contract.

### 1.2. Background

The Under Secretary of Defense for Policy (USD(P)) is an authorized position under U.S. Code Title 10, subtitle A, Part I, Chapter 4 section 134. The USD(P) is a principal staff assistant and advisor to the Secretary of Defense and the Deputy Secretary of Defense for all matters concerning the formation of national security and defense policy. The Defense Technology Security Administration (DTSA) is established as a DoD Field Activity, under the authority, direction, and control of the USD(P). The DTSA mission is to identify and mitigate national security risks associated with the international transfer of advanced technology and critical information in order to maintain the U.S. warfighter's technological edge and support U.S. national security objectives in accordance with DoD Directive 5105.72.

DTSA currently maintains an application portfolio consisting of USXPORTS suite (classified and unclassified), DOD Patent Application Review Systems (DPARS) (unclassified); Foreign Visits System (FVS) suite (classified and unclassified); National Disclosure Policy System (NDPS) (classified), Spacelink (unclassified) and other supporting applications (classified and unclassified) that reside in DoD data centers and commercial clouds (classified and unclassified) for government. Overall, DTSA has approximately 1500 users across several DoD service components and agencies, Department of State (DoS), Department of Commerce (DoC), Department of Energy (DoE), and Department of Homeland Security (DHS) that require helpdesk support and training on the DTSA applications.

### 1.3. Objectives

The objectives for the Application Management Services (AMS) are:

a. Manage, support, and operate the DTSA IT Enterprise and its users while achieving maximum cost-effectiveness, high customer satisfaction, and compliance with applicable federal laws and regulations.

b. Modernize existing applications, in accordance with DTSA's business process reengineering and cloud migration efforts. The primary goals of DTSA's application modernization efforts are to (1) leverage available techniques for automation, (2) develop and implement a cloud strategy, (3) increase overall productivity, (4) increase availability, and (5) increase speed to change. The end state will result in a DTSA data driven application environment supporting the entirety of the DTSA mission.

c. Support the transformation of DTSA into a data-centric organization through modernization of DTSA applications. This transformation will enable DTSA to perform more efficiently, boost its productivity, better engage with customers and other stakeholders, and open new opportunities. Redesigning and engineering the DTSA application environment will allow DTSA to avail of cloud-native technologies and modern data architectures, such as data lakes.

d. Maintain the security posture for all applications within the DTSA application suite consistent with DoD policy and requirements as well as industry best practices as well as preparing and evolving the enterprise to future Zero Trust architectures

## 1.4. Scope

The contractor shall perform the following services in support of the DTSA Application Management Services requirement:

5.1. Task Area 1: Basic Services
5.2. Task Area 2: Program Management
5.3. Task Area 3: Service and IT Management
5.4. Task Area 4: Enterprise IT Management
5.5. Task Area 5: Information, Knowledge Management, and Training
5.6. Task Area 6: Enhanced IT Capabilities

## 1.5. Period of Performance:

The period of performance shall be for one (1) Base Year of 12 months and four (4) 12-month option years. The Period of Performance reads as follows:

| | |
|---|---|
| Base Year | 16 March 2023 to 15 March 2024 |
| Option Year I | 16 March 2024 to 15 March 2025 |
| Option Year II | 16 March 2025 to 15 March 2026 |
| Option Year III | 16 March 2026 to 15 March 2027 |
| Option Year IV | 16 March 2027 to 15 March 2028 |

## 1.6. General Information

### 1.6.1. Quality Control

The contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor's quality control program is the means by which he assures himself that his work complies with the requirement of the contract. The Quality Control Plan (QCP) shall be delivered within 30 days after contract award. A comprehensive written QCP shall be submitted to the KO and COR within 5 working days when changes are made thereafter. After acceptance of the quality control plan the contractor shall receive the contracting officer's acceptance in writing of any proposed change to his QC system.

### 1.6.2. Quality Assurance

The government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

### 1.6.3. Recognized Holidays

Recognized Holidays are in accordance with 5 U.S.C. §6103.

| | |
|---|---|
| New Year's Day | January 1 |
| Martin Luther King Jr.'s Birthday | the third Monday in January |
| President's Day | the third Monday in February |
| Memorial Day | the last Monday in May |

| | |
|---|---|
| Juneteenth National Independence Day | June 19 |
| Independence Day | July 4 |
| Labor Day | the first Monday in September |
| Columbus Day | the second Monday in October |
| Veterans Day | November 11 |
| Thanksgiving Day | the fourth Thursday in November |

If the date falls on a Saturday, the Government holiday is the preceding Friday. If the date falls on a Sunday, the Government holiday is the following Monday. In addition to the days designated as holidays, the Government observes the following days:

- Any other day designated by Federal Statute
- Any other day designated by Executive Order
- Presidential Inauguration Day
- Any other day designated by the President's Proclamation

1.6.4. Hours of Operation

The contractor is responsible for conducting business, between the hours of 0730 and 1700 in the Eastern Time zone, Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. For other than firm fixed price contracts, the contractor will not be reimbursed when the government facility is closed for the above reasons. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential

1.6.5. Place of Performance

The majority of services shall be performed at the Mark Center, Alexandria, VA, and in Washington, DC, as well as designated Continuity of Operations (COOP) sites, as necessary. On occasion, if approved in advance by the COR, work may be performed off-site at an alternate work location at no extra cost to the Government. No services under this order shall be performed outside of the United States.

1.6.5.1. Telework

The Office of Personnel Management (OPM) recently updated its Telework Policy to allow federal employees, and contractors on site in support of federal employees, the opportunity for "unscheduled leave or unscheduled telework" in the event of hazardous road conditions in the winter months, an office move, a COOP exercise, or an emergency. This contract extends that policy to Contractors who are authorized to Telework by the COR. Authorization will be provided by the COR in writing.

The Contractor is authorized to enable contractor staff to perform off-site work when onsite presence is not required. The Contractor shall provide adequate oversight of work products to ensure contract adherence. Contractors shall have formal off-site performance policies in place if off-site performance is employed. Off-site performance arrangements on individual task orders may commence with Contracting Officer and COR approval under the following:

- Off-site performance on the part of the company is voluntary.
- Off-site performance shall not result in an increase in contract price.
- Off-site performance at personal residence, akin to federal employee telework, shall be limited to work at the Unclassified level to include Controlled Unclassified Information (CUI).
- Contractor performing off-site work is allowed (with approval) under this task order at the sole discretion of the government and may be revoked at any time.
- The Contractor is responsible for continuity of performance in accordance with the terms of the contract.
- In the event of Government closure or inability for the contractor staff to access the worksite, the decision to have the contractors ready to perform off-site in such cases will be decided upon as necessary between the Government POC and the Contractor.

Any equipment provided by the Government for off-site performance purposes will be treated as Government Furnished Equipment and guidelines in Controls for Government Property and Guidance on Removing Government Property from Government facilities shall be followed.

1.6.6. Type of Contract

The government will award a Firm-Fixed Price (FFP) contract inclusive of optional FFP CLINS.

1.6.7. Security Requirements

This contract allows for various levels of vetting to support specific PWS tasks. As specified in the DoD Contract Security Classification Specification, DD Form 254, classified work is performed under this contract. The contractor shall possess and maintain a SECRET facility clearance (FCL) at the time of proposal submission. The contractor shall provide personnel meeting the specific minimum personnel clearance (PCL) for access to support the PWS tasks.

1.6.7.1. Personnel Security

Contractor personnel performing work under this contract must possess personnel security clearance (PCL) based on an open investigation (U.S. government background investigation accepted) in accordance with the requirements in Exhibit 3 – Personnel and Labor Category Qualifications. Investigation must have favorable fingerprint results. Personnel must maintain the specified level of PCL required for the life of the contract. If an individual who has been submitted for a security clearance is "denied," receives an "Interim Declination," unfavorable fingerprint, or other than favorable adjudication, the contractor shall remove the individual from DTSA facilities, projects, and/or programs until such time as the investigation is favorably adjudicated or the individual is resubmitted and is approved. If a final determination is made that an individual does not meet or cannot maintain the minimum security requirements, the contractor shall permanently remove the individual from DTSA facilities, projects, and/or programs. All contractor and subcontractor personnel removed from facilities, projects, and/or programs shall cease charging labor hours directly or indirectly on contract/task orders.

1.6.7.2. Non-Disclosure Agreement

Contractor personnel will be required to sign a Non-Disclosure Agreement within 5 days of onboarding contract.

1.6.7.3. Physical Security

The contractor shall conform to the security provisions of 32 CFR part 117, The National Industrial Security Program Operating Manual Rule, DoD 8570.01-M, DoDI 5200.48, and the Privacy Act of 1974 for marking, handling, safeguarding, transmission/transportation, and destruction of classified and sensitive U. S. government information and material. The contractor shall be responsible for safeguarding all government equipment, information and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured per DTSA specified standard operating procedures.

1.6.7.4. Access Control

DTSA facilities and systems require a Common Access Card (CAC) for access. The COR or DTSA government sponsor will initiate CAC issuance, facility, and systems access authorization.

- Contractor personnel shall be clearly identified as a contractor while on Government property and display the CAC between shoulder and waist when on premise.
- All contractor persons engaged in work while at a Government facility shall be subject to inspection of their vehicle, identification cards, and bags/parcels at any time by the Government, and shall immediately report any known or suspected security violation to on-site security.
- The contractor shall notify the COR and appropriate DTSA security personnel within 24 hours from the time contractor employee gives notice of departure or are removed unexpectedly from contract support.
- The contractor shall assume full responsibility for proper use and security of CACs, tokens, and any other Government issued credentials and is responsible for the return of the credentials upon termination of personnel or expiration or completion of the contract/task order.

1.6.7.5. Key Control

The Contractor shall establish and implement methods of making sure all keys/key cards issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to the Contractor by the Government shall be duplicated. The Contractor shall develop procedures covering key control that shall be included in the Quality Control Plan. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The Contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the Contracting Officer.

In the event keys, other than master keys, are lost or duplicated, the Contractor shall, upon direction of the Contracting Officer, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks shall be deducted from the monthly payment due the Contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government and the total cost deducted from the monthly payment due the Contractor.

The Contractor shall prohibit the use of Government issued keys/key cards by any persons other than the Contractor's employees. The Contractor shall prohibit the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the Contracting Officer.

1.6.7.6. Lock Combinations

The Contractor shall establish and implement methods of ensuring that all lock combinations are not revealed to unauthorized persons. The Contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the Contractor's QCP.

1.6.7.7. Visit Authorization Request (VAR)

The contractor shall send a VAR via Defense Information System for Security (DISS) to the SMO DODDTSA4 for no greater than 364 days per request. Contractor personnel must have a minimum of secret access granted under the awarded CAGE code in DISS or its successor system.

1.6.7.8. Mandatory Security Training

In addition to training requirements and certifications required specific to labor category, contractor personnel (including subcontractors) regardless of security classification, shall complete required mandatory training. The contractor is responsible for verifying applicable personnel receive all required training within any specified due dates. The following table is a sample of contractor mandatory training that is subject to change per federal law, regulation, or government-wide policy:

| # | Training Course Name | Contractor Personnel Applicability |
|---|---|---|
| 1 | Active Shooter, Level 1 | All contractors |
| 2 | CDSE Operations Security (OPSEC) Training | All contractors |
| 3 | Antiterrorism Training, Level 1 | Contractors requiring routine physical access to federally controlled facilities or military installations (DFARS 252.204-7004) |
| 4 | Records Management | All contractors JSP account holders |
| 5 | DoD Cyber Awareness Challenge | All contractors JSP account holders and Personnel accessing CAC-enabled gov't sites – Authorized users of DOD information systems and networks |
| 6 | Derivative Classification | All contractors with access to classified information and authorized users of DOD classified information systems and networks |
| 7 | CDSE DoD Mandatory Controlled Unclassified Information (CUI) Training | All contractors |
| 8 | CDSE Unauthorized Disclosure (UD of Classified information and Controlled Unclassified Information (CUI) | All contractors |

| # | Training Course Name | Contractor Personnel Applicability |
|---|---|---|
| 9 | OSD CDSE Counterintelligence Awareness & Reporting | All Contractors |
| 10 | CDSE Insider Threat Awareness Training | All contractors |
| 11 | OSD/WHS Privacy Act Training | All contractors with access to PII |

1.6.8. Special Qualifications

The following requirements apply to all to the contractor and/or contractor staff.

a. The Contractor shall be a Capability Maturity Model Integration (CMMI) Level 3 for Services and Development organization upon contract award. Critically, the Contractor must have completed the Standard CMMI V2.0 Benchmark and Sustainment appraisals and provide detailed capability and performance information. The contractor must submit the following artifacts as a part of their proposal:

- CMMI V2.0 Appraisal Disclosure Statement
- CMMI V2.0 Final Findings Briefing/Report
- CMMI V2.0 Performance Report

b. The Contractor shall be required to conduct all necessary references and background checks on each of its contractor candidates that have been selected for assignment under this PWS. The reference and background check must be completed prior to the physical assignment of each contract support person to the DTSA site. In addition to conducting reference and background checks, the contractor is required to perform a thorough review of references and background investigative reports. Of note, IAT level 3 contractors must be U.S. citizens in accordance with DoD 8570.01-M. The contractor must notify DTSA of any findings that could adversely affect the contractor's personnel assignment to perform the tasks under this PWS.

c. The Contractor shall ensure that all staff possess the required qualifications to perform work as required by the U.S. Government, and that those qualifications are maintained during the life of the contract. The Contractor shall be responsible for approving individual resumes to ensure appropriate assignment of personnel to meet the requirements set forth in DoD policy. It shall be the sole responsibility of the Contractor to staff their team properly and abide by the guidelines set forth in DoD policies, procedures, and statues.

d. All contractor employees working Cyber and IT functions must comply with DoD training requirements such as those in DoDD 8140.01 and DoD 8570.01-M. Baseline security certifications are required prior to start of work with technology certifications required within six months of appointment to Cyber and IT functions.

e. Per DoD 8570.01-M and DFARS 252.239.7001, the contractor employees supporting Cyber (IA/IT) functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon contract award. All personnel assigned privileged access will maintain IAT Level I certification.

f. All contractor employees and associated sub-contractor employees must complete the DoD Cyber awareness training before issuance of IT access and each fiscal year thereafter.

1.6.9. Post Award Conference/Periodic Progress Meetings

The Contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The contracting officer, Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings the contracting officer will apprise the contractor of how the government views the contractor's performance and the contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

### 1.6.10. Contracting Officer Representative (COR)

The COR will be identified by separate letter. The COR monitors all technical aspects of the contract and assists in contract administration The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract: perform inspections necessary in connection with contract performance: maintain written and oral communications with the Contractor concerning technical aspects of the contract: issue written interpretations of technical requirements, including Government drawings, designs, specifications: monitor Contractor's performance and notifies both the Contracting Officer and Contractor of any deficiencies; coordinate availability of government furnished property, and provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

### 1.6.11. Key Personnel

The personnel specified below are key personnel and are considered to be essential to the work being performed under the resultant contract. Prior to diverting the specified individual to other projects, the contractor shall notify the Contracting Officer reasonably in advance, no less than 14 days in advance, and shall submit a written justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on the program. No diversion shall be made by the contractor without the written consent of the Contracting Officer. Noncompliance with replacement within 2 weeks of the position being vacated will be reflected negatively in past performance assessments and may be considered a material breach in the terms and conditions of the task order for which the Government may seek appropriate pecuniary remedies.

The contractor must have qualified key personnel to perform the requested services by a strong background in the following areas. The Contracting Officer or COR may request copies or evidence of qualifications used to establish that background.

Table 1:A. Key Personnel Qualifications

| # | Key Personnel | Security Requirements | Education | Certifications | Experience |
|---|---|---|---|---|---|
| 1 | Program Manager | Top Secret | 4-year degree in an IT, technology, or engineering related field | PMI Certification or ITIL Certification or Master's Degree in Program Management | Has 10 years of experience managing IT projects, at least 5 of which must be software engineering projects |
| 2 | Software Development Lead | Secret | None Identified | IAT-II Certifications IAW DoD 8570.01-M, DoD Manual – Information Assurance Workforce Improvement Program dated (dtd) 19 Dec 05 with Change 3 dtd 24 Jan 12 and Change 4 dtd 10 Nov 15 | Possess experience in the Microsoft .NET development environment including, but not limited to, VB-NET, C#, ASP.NET, Citrix, Retrievalware, Crystal Reports, Standard Query Language (SQL) and eXtensible Markup Language (XML) technologies.<br>5 or more years developing in IaaS/PaaS/SaaS environments |
| 3 | Cybersecurity Lead | Top Secret with SCI eligibility | None Identified | IAT-II Certifications IAW DoD 8570.01-M, DoD Manual – Information Assurance Workforce Improvement Program dated (dtd) 19 Dec 05 with Change 3 dtd 24 Jan 12 and Change 4 dtd 10 Nov 15 | Have experience 5 or more years with Host-Based Security Server (HBSS), Assured Compliance Assessment Solution (ACAS), Security Content Automation Protocol (SCAP) Compliance Checker (SCC), Public Key Infrastructure (PKI), anti-virus software, and securing IaaS/PaaS/SaaS cloud environments.<br>Have experience 5 or more years with RMF including roles such as the security control assessor.<br>Have experience 2 or more years with Cross Domain Solutions (CDS) in the last 5 years. |
| 4 | Data Scientist | Secret | 4-year degree in an IT, technology, or engineering related field | IAT-II Certifications IAW DoD 8570.01-M, DoD Manual – Information Assurance Workforce Improvement Program dated (dtd) 19 Dec 05 with Change | Have 5+ years of support development, enhancement and maintenance of multiple datasets.<br>Have 5+ years of programming language experience of data science technologies<br>Have 5+ years of experience with database/cloud skills |

| | | |
|---|---|---|
| | 3 dtd 24 Jan 12 and Change 4 dtd 10 Nov 15 | and data visualization skills. |

1.6.12. Identification of Contractor Employees

All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed. See section 1.6.7. Security Requirements for Credential, CAC, and badge requirements.

1.6.13. Other Direct Costs

This category includes reproduction, software licenses, specialized IT tools, and other shipping expenses associated with supporting DTSA IT operations. Some particular expenses are listed in Exhibit 5 – Estimated ODC Items.

1.6.14. Data Rights

See Solicitation/Contract FAR Clause 52.227-14 "Rights in Data-General and DFARS Clause 252.227-7015 "Technical Data-Commercial Items."

1.6.15. Organizational Conflict of Interest

Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

1.6.16. Phase in/Phase out Period

To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the Contractor shall have personnel on board, during the thirty (30) day phase in/ phase out periods. During the phase in period, the Contractor shall become familiar with performance requirements in order to commence full performance of services on the contract start date.

# PART 2
# DEFINITIONS & ACRONYMS

## 2. DEFINITIONS AND ACRONYMS

### 2.1. Definitions

2.1.1. CONTRACTOR. A supplier or vendor awarded a contract to provide specific supplies or service to the Government. The term used in this contract refers to the prime.

2.1.2. CONTRACTING OFFICER. A person with authority to enter into, administer, and or terminate contracts, and make related determinations and findings on behalf of the Government. Note: The only individual who can legally bind the Government.

2.1.3. CONTRACTING OFFICER'S REPRESENTATIVE (COR). An employee of the U.S. Government appointed by the contracting officer to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.4. DATA ACQUISITION. The set of activities performed to identify and obtain data, or have access to it under either limited or unlimited rights for use.

2.1.5. DATA ANALYSIS. The set of activities performed to study and present data to extract information and knowledge.

2.1.6. DATA LAKES. A collection of storage instances of various data assets additional to the originating data sources that allows an organization to store all of their data, structured and unstructured, in one centralized repository.

2.1.7. DATA LIFECYCLE MANAGEMENT. A data lifecycle is a conceptualization that captures the stages of data, from creation to destruction. Stages within the data lifecycle often include Data Acquisition, Data Maintenance and Storage, Data Staging, Data Analysis, Data Usage, and Data Retirement.

2.1.8. DATA MAINTENANCE AND STORAGE. The set of activities performed to organize and curate data in order to make it available for future use.

2.1.9. DATA RETIREMENT. The set of activities performed to identify data that is no longer needed and to appropriately remove it from active data sets.

2.1.10. DATA STAGING. The set of activities performed when moving data into intermediate storage as preparation for analysis. These activities often include data quality improvement, structure or format changes, and partitioning of attributes into similar subsets.

2.1.11. DATA USAGE. The set of activities performed to communicate the information that the data collectively contain.

2.1.12. DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the Performance Work Statement.

2.1.13. DELIVERABLE. Anything that can be physically delivered, but may include non-manufactured things such as meeting minutes or reports.

2.1.14. ESSENTIAL PERSONNEL: Employees who are critical to the continuation of key operations and services that directly relate to the work being performed under the resultant contract.

2.1.15. INFRASTRUCTURE AS A SERVICE. A type of cloud computing service that offers essential compute, storage, and networking resources on demand, on a pay-as-you-go basis.

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

2.1.17. PERSONNEL: Employees of the contractor, or any subcontractor(s), partners, or team members, and consultants engaged by any of those entities.

2.1.18. PHYSICAL SECURITY. Actions that prevent the loss or damage of Government property.

2.1.19. PLATFORM AS A SERVICE. A type of cloud computing service that allows for complete development and deployment environment in the cloud, with resources that enable delivery of everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications.

2.1.20. QUALITY ASSURANCE. The Government procedures to verify that services being performed by the contractor are performed according to acceptable standards.

2.1.21. QUALITY ASSURANCE Surveillance Plan (QASP). An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance.

2.1.22. QUALITY CONTROL. All necessary measures taken by the contractor to assure that the quality of an end product or service shall meet contract requirements.

2.1.23. ROBOTIC PROCESS AUTOMATION. Robotic process automation is a form of business process automation technology based on metaphorical software robots or on artificial intelligence /digital workers.

2.1.24. SOFTWARE AS A SERVICE. A type of cloud computing service that allows for users to connect to and use cloud-based apps over the Internet.

2.1.25. SUBCONTRACTOR. One that enters into a contract with a prime contractor. The Government does not have privity of contract with the subcontractor.

2.1.26. WORK DAY. The number of hours per day the contractor provides services in accordance with the contract.

2.1.27. WORK WEEK. Monday through Friday, unless specified otherwise

2.1.28. ZERO TRUST. An approach for providing secure access to data and services for all active entities in an enterprise (e.g., users, hardware, and services) centering on assuring the confidentiality and integrity of data in applications by providing secure access to data and services for all active entities in an enterprise (e.g., users, hardware, and services).

## 2.2. Acronyms

| | |
|---|---|
| ACAS | Assured Compliance Assessment Solution |
| ACCM | Asset Configuration Compliance Module |
| ACOR | Alternate Contracting Officer's Representative |
| AI | Artificial Intelligence |
| AO | Authorizing Official |
| APL | Approved Products List |
| BCTF | Boards, Commissions, and Task Forces |
| BPM | Business Process Management |
| C5ISR | Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance |
| CAC | Common Access Card |
| CAGE | Commercial and Government Entity |
| CCB | Configuration Control Board |
| CCE | Center for Credentialing & Education |
| CCRI | Command Cyber Readiness Inspection |
| CDO | Chief Data Officer |
| CDS | Cross Domain Solution |
| CFR | Code of Federal Regulations |
| CI | Configuration Item |
| CR | Change Request |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CMMI | Capability Maturity Model Integration |
| CMP | Change Management Plan |
| CMP | Configuration Management Plan |
| CNSS | Committee on National Security Systems |
| COOP | Continuity of Operations Plan |
| CONUS | Continental United States (excludes Alaska and Hawaii) |
| COR | Contracting Officer Representative |
| COTR | Contracting Officer's Technical Representative |
| COTS | Commercial-Off-the-Shelf |
| CPARS | Contractor Performance Assessment Reporting System |
| CSSP | Cyber Security Service Provider |
| CT&E | Certification, Test & Evaluation |
| CUI | Controlled Unclassified Information |
| DD Form 254 | DoD Contract Security Classification Specification |
| DFARS | Defense Federal Acquisition Regulation Supplement |
| DISA | Defense Information Systems Agency |
| DLA | Defense Logistics Agency |
| DMAIC | Define, Measure, Analyze, Improve, and Control |
| DMDC | Defense Manpower Data Center |
| DOD | Department of Defense |
| DODD | Department of Defense Directive |
| DODIN | DoD Information Network |
| DoE | Department of Energy |
| DoS | Department of State |
| DRP | Disaster Recovery Plan |
| DTSA | Defense Technology Security Administration |
| ECD | Export Control Directorate |
| EIA | Electronic Industries Alliance |
| FAR | Federal Acquisition Regulation |

| | |
|---|---|
| FCL | Facility Security Clearance |
| FISMA | Federal Information Security Management Act |
| FTR | Federal Travel Regulations |
| GSA | General Service Administration |
| GOTS | Government Off-The-Shelf |
| GTM | Government Technical Monitor |
| HBSS | Host-Based Security Server |
| HIPAA | Health Insurance Portability and Accountability Act of 1996 |
| IA | Information Assurance |
| IaaS | Infrastructure as a Service |
| IAVA | Information Assurance Vulnerability Alerts |
| IAVM | Information Assurance Vulnerability Management |
| IAW | In Accordance With |
| IEC | International Electrotechnical Commission |
| IED | International Engagement Directorate |
| IEEE | Institute of Electrical and Electronics Engineers |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| ITIL | Information Technology Infrastructure Library |
| ITSM | IT Service Management |
| IV&V | Independent Verification and Validation |
| JSP | Joint Service Provider |
| KO | Contracting Officer |
| MD | Management Directorate |
| ML | Machine Learning |
| NARA | National Archives and Records Administration |
| NDAA | National Defense Authorization Act |
| NDPS | National Disclosure Policy System |
| NIAP | National Information Assurance Partnership |
| NIPRNET | Non-classified Internet Protocol Router Network |
| NIST | National Institute of Standards and Technology |
| NLT | No Later Than |
| OCI | Organizational Conflict of Interest |
| OCIO | Office of the Chief Information Officer |
| OCONUS | Outside Continental United States (includes Alaska and Hawaii) |
| ODC | Other Direct Costs |
| O&M | Operations and Maintenance |
| OPM | Office of Personnel Management |
| OPSEC | Operations Security |
| OSD | Office of the Secretary of Defense |
| PaaS | Platform as a Service |
| PBO | Property Book Officer |
| PCL | Personnel Security Clearance |
| PDCA | Plan-Do-Check-Act |
| PENCERT | Pentagon Computer Emergency Response Team |
| PENCIRT | Pentagon Computer Incident Response Team |
| PIPO | Phase In/Phase Out |
| PKI | Public Key Infrastructure |
| PMI | Project Management Institute |
| PMP | Project Management Professional |
| POA&M | Plan of Action and Milestone |
| POC | Point of Contact |
| PRS | Performance Requirements Summary |
| PWS | Performance Work Statement |
| QA | Quality Assurance |
| QAP | Quality Assurance Program |

| | |
|---|---|
| QASP | Quality Assurance Surveillance Plan |
| QC | Quality Control |
| QCP | Quality Control Program |
| RACI | Responsible, Accountable, Consulted, and Informed. |
| RMF | Risk Management Framework |
| RPA | Robotic Process Automation |
| RUP | Rational Unified Process |
| SaaS | Software as a Service |
| SCAMPI | Standard CMMI Appraisal Method for Process Improvement |
| SCAP | Security Content Automation Protocol |
| SCC | SCAP Compliance Checker |
| SCI | Sensitive Compartmented Information |
| SDLC | Software Development Life Cycle |
| SECDEF | U. S. Secretary of Defense |
| SEF | Systems Engineering Framework |
| SIPRNET | Secret Internet Protocol Router Network |
| SPAN | Security Policy Automation Network |
| SOP | Standard Operating Procedure |
| SQL | Standard Query Language |
| ST&E | Security, Test & Evaluation |
| STIG | Security Technical Implementation Guide |
| TE | Technical Exhibit |
| USAF | United States Air Force |
| USCYBERCOM | United States Cyber Command |
| USD(P) | Under Secretary of Defense for Policy |
| USG | United States Government |
| VM | Virtual Machine |
| WHS | Washington Headquarters Services |
| XML | eXtensible Markup Language |
| ZT | Zero Trust |
| ZTA | Zero Trust Architecture |

# PART 3

# GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

## 3. GOVERNMENT FURNISHED ITEMS AND SERVICES

### 3.1. Facilities, Equipment, and Material

DTSA will provide all needed hardware, software, and furniture (standard desk/cubicle, chair, etc.) for personnel working on-site at the facility. In the event that off-site work is approved by the COR, the DTSA will provide the appropriate level of remote access based on the requirements specified in section C, and the specific tasks each individual is performing. Any remote access that is granted will be in strict accordance with all applicable DTSA and Federal Government requirements (IT Security, mandatory training, etc.).

DTSA will provide a suitable working area including desks, chairs, storage for documentation, telephones with access to outside lines, connectivity to the DTSA local area network for government furnished computer and a printer for personnel working onsite. DTSA will provide access to facilities and personnel as required for completion of activities associated with this contract.

### 3.2. Utilities

The Government will provide utilities (e.g. electricity, water and sewer, network access) at facilities authorized for performance of tasks outlined in this PWS. The Contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities, which include turning off the water faucets or valves after using the required amount to accomplish cleaning vehicles and equipment.

# PART 4

# CONTRACTOR FURNISHED ITEMS AND SERVICES

## 4. CONTRACTOR FURNISHED ITEMS AND RESPONSIBILITIES

### 4.1. General

The Contractor shall furnish all supplies, equipment, facilities and services required to perform work under this contract that are not listed under Part 3 of this PWS.

### 4.2. Security Clearance

The contractor shall possess and maintain a TOP SECRET security facility clearance from the Defense Counterintelligence and Security Agency (DSCA) at the time of proposal submissions. The DD 254 is provided as an attachment.

**PART 5**

**SPECIFIC TASKS**

## 5. SPECIFIC TASKS

SPECIFIC TASKS TABLE OF CONTENTS



### 5.1. Task Area 1: Basic Services

#### 5.1.1. Basic Task Standards

Throughout this PWS the following tasks and requirements are expected. The contractor shall:

5.1.1.1. Comply with all Federal, DoD and DTSA instructions, policies, regulations and guidelines including, but not limited to those that affect IT, cybersecurity, information security, and physical security.

5.1.1.2. Ensure all PWS tasks are conducted in harmony and synchrony such as to produce a seamless IT Enterprise.

5.1.1.3. Deploy and implement technologies, processes, and procedures by maximizing value and minimizing cost of ownership within the DTSA IT Enterprise.

## 5.2. Task Area 2: Program Management

### 5.2.1. Program Management Planning

DTSA desires a Contract Program Manager be the primary liaison to the Government for all areas associated with this contract as well as manage the work schedules and activities performed by the contract employees. In addition to providing this liaison, the contractor shall:

5.2.1.1. Develop, execute and operate under a U.S. Government-approved Project Management Plan (PMP), comprehensively updated throughout the performance period as changes occur. The PMP will address all PWS tasks and contractor projects.

5.2.1.2. Develop and maintain a Staff/Resource Management Plan that tracks certification, qualifications, labor categories, security clearances, task assignments, for all contract personal, inclusive of key personnel.

5.2.1.3. Develop, execute and operate project-specific PMPs for short term projects that arise over the course of the PWS. project-specific PMPs will include requirements, specification, schedule, progress, costs and expenditures and other elements as necessary.

5.2.1.4. Develop, execute and operate Program Management Plan and/or Service Management Plans for each major application and service provided via this PWS for DTSA application and family of applications. Plans will show how each subject will be sustained, maintained, and supported.

### 5.2.2. Status Reporting

DTSA desires a robust and broad range of reporting and metrics on program, project, and contract health and performance. The contractor shall provide this data in the form of monthly, daily and quarterly reports in support DTSA and its IT Enterprise for internal and external use by DTSA. The contractor shall:

5.2.2.1. Prepare and present a Monthly Information Technology Program Report that captures or summarizes completed tasks, staffing status, financials (to include labor, travel and equipment ODC funds), and any issues/challenges encountered. Report may expand to measure and include any task or attribute of the PWS per COR/GTM direction.

5.2.2.2. Develop a SOP for Daily Application and Capability Health Reporting that describes how to determine availability of each DTSA IT Enterprise application and capability from the perspective of a DTSA user.

5.2.2.3. Provide Daily Application and Capability Health Reports in accordance with SOP.

5.2.2.4. Develop a SOP for Monthly Network Availability Performance Metrics Report. Report must include physical and virtual network equities within the DTSA IT Enterprise.

5.2.2.5. Provide Monthly Network Availability Performance Metrics Report in accordance with SOP.

### 5.2.3. Change Management Support

DTSA operates a diverse interagency change management ecosystem. The agency requires the contractor to provide support for all change management and configuration management activities inclusive of hosting meetings, preparing briefs, support backlog curation, and maintenance and development of management documentation. Additionally, the change management will be the chief process by which changes to DTSA applications are modified. The contractor shall:

5.2.3.1. Develop and maintain a charter for each CCB hosted by DTSA including both internal and external CCBs in accordance with DTSA CIO Change Management Vision.

5.2.3.2. Develop and maintain a Change Management Plan for the agency-level and each CCB hosted by DTSA, including both internal and external CCBs in accordance with DTSA CIO Change Management Vision.

5.2.3.3. Host, schedule, and record regular CCB meetings including sending invites, developing agendas, and briefing materials for each CCB.

5.2.3.4. Establish, define, and present a framework for estimating complexity, cost, and risk as well as development and implementation time of backlog change requests. This task includes developing and delivering training materials for DTSA and partner agency consumption.

5.2.3.5. Facilitate and shepherd change requests through DTSA organizational change management processes.

5.2.3.6. Conduct investment and development analysis for change requests using established procedures.

5.2.3.7. Curate a list of all change requests and their status.

5.2.4. Configuration Management

DTSA seeks a comprehensive Configuration Management program with intent to track all attributes of its IT enterprise. The contractor shall:

5.2.4.1. Develop and maintain a Configuration Management Plan (CMP), which describes the Configuration Management Program, including responsibilities, methodology and procedures for baseline identification, configuration control, and audit and status accounting of all configuration items.

5.2.4.2. Track and establish all configuration items and baselines including but not limited to applications, software, hardware, services, clouds elements, source code, source code release versions, source code documentation, system configurations, and schemas. Configuration items will be marinated and stored in COR/GTM approved libraries or repositories.

5.2.4.3. Ensure configuration management and Change Management processes have appropriate interfaces for efficient operations.

5.2.5. Program Management Support

DTSA seeks program management support for its IT Enterprise. The support will establish (as needed) and maintain a program management information system (PMIS) and service catalog and library for all tasks and projects within the DTSA OCIO and IT and Cybersecurity Division and its partners. The contractor shall:

5.2.5.1. Establish (as needed) and maintain a PMIS for or all tasks and projects within the DTSA OCIO and IT and Cybersecurity Division and its partners. Establish (as needed) and maintain a PMIS for or all tasks and projects within the DTSA OCIO and IT and Cybersecurity Division and its partners. Tools utilized are expected already be in use and/or available to DTSA.

5.2.5.2. Draft and maintain training and user guides for all DTSA OCIO and IT and Cybersecurity Division government and contractor personnel to contribute and use the PMIS.

5.2.6. Metrics and Evaluation

DTSA requires comprehensive telemetry to assess the health and performance of its IT enterprise. The contractor shall:

5.2.6.1. Develop and maintain an Evaluation Plan that proposes measures to show application health including but not limited to application and application module usage, availability, response time, various transaction quantities and other key performance indicators. The plan must include processes to update and add new measures as requested and must also include reporting requirements aggregated through this PWS. Reporting frequency must monthly or more frequently.

5.2.6.2. Implement approved Evaluation Plan.

5.2.6.3. Conduct regular review of the Evaluation Plan. Continually conduct performance benchmarking activities through the evaluation of existing operations or processes and data, and provide recommendations of proposed operations/processes, data baselines, and interfaces

5.2.6.4. Collect and report metrics on each application maintained under this contract on an on-demand and monthly basis

5.2.7. Contract Transition

DTSA expects a Contract Kick Off Meeting. The meeting will provide an introduction between contractor and U.S. Government personnel who will be involved with the activities addressed in the PWS. The meeting will provide an opportunity to discuss technical, management, personnel and cyber security topics, travel authorization and reporting procedures. At a minimum, the attendees shall include key contractor personnel, relevant U.S. Government personnel, and the COR. The contractor shall:

5.2.7.1. Develop and provide Contract Kick-Off Agenda and Briefing Slides

5.2.7.2. Provide kick off contract transition plan addressing, at a minimum: Roles and responsibilities, Points of Contacts (including key personnel), Task order transitioning process and timeframes, and review of contractor approach.

5.2.7.3. Develop an end-of-contract transition plan. Plan is to perform full migration within a 60-day period with coordination with the follow on service provider. A timeframe target period of no more than five days for validated migration of each application server and associated database server, including test and development servers to the cloud environment. Coordinate all impacts to system availability impacts during the 60-day migration period for the migration and subsequent cutover to the service provider infrastructure and secure approval from the Contracting Officer Representative (COR) before execution.

## 5.3. Task Area 3: Service and IT Management

### 5.3.1. Managed Services

DTSA utilizes numerous agreement and acquired services to deliver its IT Enterprise. DTSA expects the contractor to support and manage those services for DTSA. The contractor shall:

5.3.1.1. Develop and maintain a SOP for the management of Managed Services. SOP must also drive examination of services and capabilities provided by enterprise providers and internally within DTSA to ensuring there is limited duplication of these services by DTSA and enterprise capability is used to its maximum benefit.

5.3.1.2. Manage accounts and portfolios of managed IT services directly and on behalf of DTSA in accordance with approved SOP. Services may include cloud, applications, computer/serve room production capacity, application maintenance, configuration management, network support, performance monitoring and tuning, system backup and recovery, database management, storage management, data protection and management, help desk, system operations, infrastructure facilities, and information security/cybersecurity.

5.3.1.3. Seek and implement, with government approval or as directed, methods to reduce costs or increase value with managed services.

### 5.3.2. Acquisition

DTSA requires the support in acquisition of IT software, hardware, and services. The contractor shall:

5.3.2.1. Develop, maintain, and execute a process and procedure for the acquisition of IT. Included in the process must be processes for identifying and evaluating existing and new Commercial-Off-the-Shelf (COTS) or Government Off-The-Shelf (GOTS) solutions.

5.3.2.2. Support the U.S. Government in the acquisition of software including, but not limited to, applications, operating systems, and licenses. This includes providing complete solutions for all software including any components necessary for integration.

5.3.2.3. Support the U.S. Government in the acquisition of commodity IT equipment including, but not limited to, servers, central processing units (CPU), disks, disk drives, display screens, keyboards, printers, boards, memory, chips, tapes and tape drives, secure wireless solutions, hubs, transceivers, terminal servers, desktop and laptop computers, personal digital assistants (PDA) and ancillary peripheral hardware. Hardware delivered under this contract, as appropriate, shall include all controllers, connectors, cables, drivers, adapters and other associated hardware and software required for operations, as provided by the original equipment manufacturer.

5.3.2.4. Ensure all acquisitions made under this contract use General Services Administration (GSA) schedules as sources of supply and, for software, via Enterprise Software Agreements.

5.3.2.5. Provide justification and acquire COR approval for any acquisitions to be made without the use of the GSA schedules.

5.3.2.6. Manage software license agreements for leveraged suppliers, exploiting the agreement and optimizing software expenses, while remaining compliant with the agreements terms and conditions. This includes supporting agreement summary information such as general terms and conditions, benefits, strategic and tactical directions, license ordering information, internal billing process, pricing and deployment and support of the products included in the agreement.

5.3.2.7. Provide reports on all acquisitions including license agreements, inventory, utilization, age, vendor support and other related details.

5.3.2.8. Provide quotes on hardware, software, services, and related capabilities.

5.3.3. Market Research and Prototyping

DTSA seeks comprehensive and thorough Market Research and Prototyping support in seeking new technologies and capabilities for its enterprise. The contractor shall:

5.3.3.1. Provide definition, development, tailoring, installation, testing, evaluation, operation, and training of prototype systems and services. This support can cover the entire life-cycle of a prototype from initial knowledge engineering and user requirements identification through prototype evolution to provide an operational product that supports evolving mission requirements.

5.3.3.2. Identify internal and external, current and potential service provider and supplier requirements, such as hosting resources, vulnerability testing, and DTSA IT enterprise integrations needs.

5.3.3.3. Determine and document solutions regulatory compliance and evaluation status such as National Information Assurance Partnership (NIAP)-approved as well as on DISA's Approved Products List (APL).

## 5.4. Task Area 4: Enterprise IT Management

5.4.1. Enterprise IT Policy and Planning

DTSA requires management, expertise and execution, through all software and system development lifecycle stages of its IT enterprise inclusive of its mission applications. This also includes support and development of IT strategy, roadmaps, polices, plans, standards, processes, procedures, and other documents and artifacts the affect DTSA and its interagency partners. The contractor shall:

5.4.1.1. Develop, maintain, and support IT strategy, roadmaps, polices, plans, standards, processes, procedures and other documents and artifacts consistent with all the DoD IT Enterprise Strategy and DoD Information Enterprise Architecture as well as other strategies (e.g. Zero Trust, Data, Cloud, etc) policies, directives, and other Federal and department-wide direction. Additionally, inputs shall include organizational analyses, market studies, alternative analyses, feasibility studies, technology evaluations, and cyber threat analyses.

5.4.1.2. Support DTSA's transformation into a data-centric organization. Develop, maintain, and implement a Data Strategy and Plan for all DTSA mission applications, adhering to national and DoD Data strategy requirements, principles, capabilities and needs. Additionally, the strategy must address data lifecycle management, inclusive of data acquisition, data maintenance and storage, data staging, data analysis, data usage, and data retirement stages as well as properties of data resilience. The strategy must also address incorporation of a data lake into the DTSA IT Enterprise with maximized utility across all of its environments. Elements of the Data Strategy and Plan must be distilled into increments that may be implemented via the change management processes in this PWS. Solutions shall be proposed to the COR/GTM for approval and must take advantage of enterprise tools to the greatest extent possible.

5.4.1.3. Develop a modernization plan for government approval to update and upgrade DTSA mission applications from monolithic client-server applications to an application environment that utilizes and leverages current technologies and design patterns (e.g. Agile, DEVSECOPS, cloud, robotic process automation, machine learning, artificial intelligence, micro-services, etc.). The plan must be a "living document", updated regularly to include state of the art and technology upgrades as they become available or desired by DTSA. Modernization efforts shall focus on (1) increasing the degree of automation, (2) realizing the potential of cloud-based techniques, (3) generally increasing performance, (4) ensuring high availability, and (5) increase speed to change. The plan shall be compartmentalized such that it can be executed iteratively in as small increments as possible and practical (e.g. two-week sprints) and thus be integrated into the change management processes in this PWS.

5.4.1.4. Develop, maintain, and execute a cloud services delivery strategy for government approval to meet the needs of DTSA. The plan shall advance current DTSA mission applications and future application environment from Infrastructure as a Service (IaaS) models to Platform as a Service (PaaS) and Software as a Service (SaaS) models to the greatest extent possible and practical.

5.4.1.5. Provide the skillsets required to upgrade DTSA IT Enterprise technology. Upgrades must increase business functionality, reengineer a business function, keep current with vendor upgrades or when upgrading existing technology. Technology transformation may be accomplished by evolving, converting/migrating legacy applications to a new technology either with or without new business functionality or it may include introducing new technology into DTSA's IT enterprise. Support activities include assessments of the current application portfolio, evaluation of the technology assets before beginning technology transformation and business case development for justification of an initiative. Also included are: technology transformations, which may include, appropriate return on investment, benchmarks and milestones. The following activities may also be included: planning, analysis, requirements development, proof of concept, deployment, implementation, integration, remediation, data migration, documentation, application programming and support services; and training support.

5.4.2. Requirements Analysis

DTSA requires regular requirements gathering and analysis for its IT Enterprise and Business. The contractor shall:

5.4.2.1. Leverage data collection tools, conduct surveys, hold meetings with customers, analyze data, to consolidate and refine organizational requirements.

5.4.2.2. Consolidate and refine all requirements to assist in synthesizing interagency and organizational requirements into actionable items that lead to the design, development, test, validation and deployment of affordable application and database upgrades.

5.4.2.3. Gather government approved requirements and develop and maintain specification documentation (to include requirement traceability and other supporting requirement documents) for all DTSA IT enterprise applications, services, capabilities, and projects.

5.4.2.4. Research, design, build (using best of spiral and incremental technology development approaches) document, test, certify, and validate DTSA applications stay on the leading edge of new technologies.

5.4.3. Application Development, Enhancement, and Customization

DTSA requires regular application development functions as part of this PWS, inclusive, but not limited to application enhancements and "bug" fixes. All development must comply with Federal and DoD strategies, polices, and related artifacts as well as utilize industry leading best practices. Requests will typically be queued into a set of backlogs via change management processes in this PWS. The contractor shall:

5.4.3.1. Develop, maintain, and implement SOPs for coding, developing, designing, customization, testing, deploying, patching, upgrading and maintaining applications and supporting architectures IAW applicable Government standards. The SOP is expected to be integrated throughout all areas of the PWS. The SOPS will also implement current and secure technologies and design patterns (e.g. Agile, DEVSECOPS, Zero Trust, cloud, robotic process automation, machine learning, artificial intelligence, micro-services, etc.) and will be regularly updated to maintain currency. SOP will drive creation of necessary security documentation (e.g. RMF) as well. DTSA expects development practices to evolve towards a Continuous Integration and Continuous Delivery (CICD) pipelines.

5.4.3.2. Execute all stages of software and system lifecycles, in accordance with approved SOP, including planning, developing, designing, customization, testing, deploying, patching, upgrading, maintaining, and fixing of new and existing application capability. This does include programming of application code, management, development and changes to databases and data structures, as well as modification and change to on-prem cloud based infrastructure and platform as a service integration to perform and/or automate business functions.

5.4.3.3. Document all development, deployment, projects, associated resourcing, and any maintenance updates of mission applications. This includes any requisite documentation of those activities (e.g. Release information, Change logs, RMF documentation).

5.4.3.4. Provide requirements analysis and documentation of requirements and project plans for mission applications by working with user representation and other DTSA stakeholders to define and capture those requirements.

5.4.3.5. Develop and implement a mission application development methodology/process(es) to gather requirements and deliver products to the customer using industry best practices and in concert with DTSA change management processes, while ensuring quality and timeliness of the delivery.

5.4.3.6. Migrate and transition applications, associated data, code, management responsibilities and other associated element into or out of the JSP, DoD, or Commercial hosting environments, implementation models, and service providers as required (e.g. IaaS, PaaS).

5.4.3.7. Plan, conduct, and document testing to determine if the solutions meet functional, performance, and security requirements.

5.4.3.8. Plan, develop, and implement approved deployment solutions and procedures for build releases for DTSA IT Enterprise Applications and capabilities.

5.4.3.9. Plan and execute post-deployment strategies and services to correct issues or to implement additional application phases.

5.4.3.10. Prepare and maintain variety of application documentation consistent with industry leading practices and DTSA business processes to document the solutions for the purposes of security, future enhancement, maintenance, and approval for release. This also includes data dictionaries, and other artifacts that describe the DTSA IT Enterprise.

5.4.3.11. Develop and maintain a plan to identify opportunities to apply robotic process automation (RPA) technologies for near and long term DTSA business process and IT modernization efforts. The desired outcome is to reduce the need for human experts to spend time on mundane repetitive tasks.

5.4.3.12. Develop, maintain, end execute a plan to identify opportunities for applying machine learning (ML) and artificial intelligence (AI) technologies for near and long term DTSA business process and IT modernization efforts.

5.4.4. IT Operations and Support

DTSA requires complete administration and operational support of its IT Enterprise. As indicated in all tasks in the PWS, IT Operations and Support must blend organically and transparently to ensure seamless execution. The contractor shall:

5.4.4.1. Develop IT Operations SOP that addresses all task related to the operations and maintenance of all DTSA enterprise and non-enterprise applications, enterprise consolidated non-production and production hosting environments, servers, services, storage systems networks (physical or virtual) and systems. SOP needs to ensure compliance with all applicable DoD policies (e.g.: STIGS, SRGs, etc) and industry best practices. SOP shall also include reporting and metrics for IT Operations Health.

5.4.4.2. Administer and operate in accordance with approved SOP, all DTSA enterprise and non-enterprise applications, enterprise consolidated non-production and production hosting environments, servers, services, storage systems networks (physical or virtual) and systems. Continual identification of ways to improve administration and operations techniques and resources is expected.

5.4.4.3. Liaise and coordinate with network service providers on all network, virtual, physical, or otherwise, related matters/projects, including activation of subnetworks (e.g., test, development, operational, DMZ), firewall ruleset requests, and additional project requests, as required. Ensure that the DTSA IT Enterprise, including mission applications and collaboration environments, are operational at least 90% of the time to all authorized end users and customers.

5.4.4.4. Execute all tasks related to installation, configuration, maintenance, and upgrade for all servers, systems, clouds, and appliances, including virtual and physical instances. This includes but is not limited to managing the resources and activities for domain controllers, member servers and appliances, permissions, user account information, activation, deactivation, authentication, and enforcement of DoD security policies. Member servers and appliances that the contract shall manage include functions and purposes such as file, print, email, cloud, web, application, database, proxy, firewall, storage, certificate, and remote access servers.

5.4.4.5. Design and maintain databases at DTSA including database architecture, database structures, and data dictionaries. Additionally, perform data recovery, cloud, and tape backup operations, as well as evaluate and recommend improvements to the cybersecurity posture of all DTSA databases and data applications. DTSA also requires that database monitoring, troubleshooting, performance tuning, repair, backup and restoration as well as database patches installation and upgrades be conducted.

5.4.4.6. Identify, plan, implement, test, and maintain data storage plans, process, and solutions for DTSA IT including physical, virtual, and cloud capabilities.

5.4.4.7. Create, manage, and archive web folders and databases utilizing existing DTSA tools as required.

5.4.4.8. Plan and Provide equipment installation for IT equipment directly managed by DTSA. This includes special use equipment (e.g. SIPR and NIPR transfer workstations, client machines used to access the NESSUS servers), and desk side IT equipment on other domains (e.g., Commercial domain).

5.4.4.9. Provide and execute as a single-engagement/control point for IT issue resolution. The includes taking action to resolve and implement LAN configuration issues and equipment hookups; analyze, isolate and coordinate corrective action for communications-related problems; and the configuration of communications equipment in support of these environments. Outages and Degradation Issues must be resolved efficiently with minimal down time. All network modifications and configuration changes are properly documented. Outages and Degradation Issue resolution must include dynamic, final, and after action reports including lessons learned.

5.4.4.10. Develop SOP for Application Operations Report. SOP must address data sources and steps to produce report.

5.4.4.11. Provide Application Operations Report in accordance with SOP.

5.4.4.12. Develop SOP for Storage Optimization Report. SOP must address data sources and steps to produce report.

5.4.4.13. Provide Storage Optimization Report in accordance with SOP.

5.4.5. Business Continuity Support

DTSA desires Business Continuity Support from its IT Enterprise. This includes a full range of expert technical input and technology capability. The contractor shall:

5.4.5.1. Design, develop, maintain and implement IT Continuity of Operations Plan (COOP), Disaster Recovery Plan (DRP) and capabilities throughout the DTSA IT Enterprise using enterprise and non-enterprise solutions. Participate in designing and implementing failover capabilities which may be at the hardware/software level at an alternate site. Capability restoration must be possible within 24 hours.

5.4.5.2. Develop and execute tests of all availability-enabling capabilities. This includes testing restoration of backups and rolling back virtual machines. Tests must be approved by COR/GTM and may be waived/delayed by COR/GTM. Tests may use sampling if approved by COR/GTM.

5.4.5.3. Develop and/or provide inputs on IT Continuity of Operations Plan (COOP).

5.4.5.4. Develop and/or provide inputs on Disaster Recovery Plan (DRP).

5.4.6. Service Desk

DTSA expects operation and staffing of a DTSA Mission Application service desk. The service desk will function as a single point of contact for problem identification, incident management, ticket routing and resolution to support customers and will utilize a trouble-ticket system that can track workflows, severity level, and route tickets to the appropriate Tier I, II and III technician for resolution. The contractor shall:

5.4.6.1. Provide full-time, on-site, Tier I (basic technical support) support staff at DTSA to provide telephonic, face-to-face, and email collaboration with customers and users. Additionally, provide Tier II (In-depth technical support) and Tier III (Expert product and service support) level application support service desk services.

5.4.6.2. Develop and maintain processes and procedures designed to facilitate the management of the service desk including arrangement of service tiers and how requests and tickets are route between service tiers.

5.4.6.3. Maintain a IT Service Management (ITSM) System to track workflows, severity level, and route tickets to the appropriate Tier I, II and III, technician for resolution.

5.4.6.4. Develop and execute process and procedures grant, modify, and remove individual application, application resource, web folder, and database permissions.

5.4.6.5. Provision, modify, and decommission application role-based user accounts and access

5.4.6.6. Conduct and implement user, server and object certificates and PKI process and other identification and authentication infrastructure support as required. This includes coordination with DTSA service providers to implement procedures to request, maintain, store, distribute, revoke, and upgrade Class 1, 2, and 3 digital certificates. Performing PKI, certificate, token, and authenticator roles for DTSA users is expected.

5.4.6.7. Complete forms for Server Certificates.

5.4.6.8. Provide User Access Report showing quantities of accounts in total as well as those added, deleted, and or changed for each resource with the DTSA IT Enterprise. Report must also list similar metrics for Certificate, token, and authenticators issued or revoked.

5.4.6.9. Provide reports on Service Desk performance.

5.4.7. Cybersecurity and Compliance

DTSA seeks complete and compliant cybersecurity support and integration across its IT enterprise, including mission applications. As indicated in all tasks in the PWS, Cybersecurity must have blended organically and transparently to ensure seamless execution. The contractor shall:

5.4.7.1. Develop and implement a comprehensive Risk Management Framework Implementation at DTSA integrating all current policy at the Federal and DoD level including provisions for continuous authorization and continuous monitoring, increasing efficiency where ever possible.

5.4.7.2. Develop and implement a RMF Process and Workflow system (e.g. eMASS/ERS). System must be able to report on health indicators of RMF packages and systems including, but not limited to, POAMs and authorizations statuses.

5.4.7.3. Support, apply, and conduct RMF processes for all DTSA IT enterprise equities and applications to ensure they maintain their cybersecurity posture throughout the system's life cycle. This includes contributing to or performing roles as Information System Security Manager/Officer and Security Control Assessor to produce and maintain documents, testing, analysis, Plans of Action with Milestones, security plans, results of security control assessments, supporting security artifacts (i.e., network/enclave security architectures), memoranda, and other artifacts required for the process.

5.4.7.4. Prepare, deliver, and maintain RMF POAMs for each DTSA IT Enterprise Application by authorization boundary.

5.4.7.5. Resolve POAM vulnerabilities on all DTSA IT Enterprise applications, systems, and enclaves. Resolution may be captured via RMF POAM maintenance.

5.4.7.6. Support and participate in all IT audits, inspections, and evaluations of the DTSA IT Enterprise.

5.4.7.7. Operate all DTSA IT Enterprise equites in an inspection ready posture. This means maintenance operating regular self-inspection, review, and implementation compliance requirements for all DoD cyber inspections and evaluations such as Command Cyber Readiness Inspection (CCRI), Command Cyber Operational Readiness Inspection (CCORI), DoD Cyber Security Service Provider (CSSP) and any successor programs as well as those directed from or sponsored by U.S. Cyber Command (USCYBERCOM Joint Force Headquarters-Department of Defense Information Networks (JFHQ-DoDIN), Defense Information Systems Agency (DISA), or Joint Service Provider (JSP)

5.4.7.8. Complete Cyber Inspection Action Items, close findings, and update related inspection POAMs.

5.4.7.9. Maintain and submit DTSA DoD Cyber Scorecard and any related or successor reports, scorecards, repositories, or systems of record (e.g., Continuous Monitoring and Risk Scoring). DoD cyber scorecards provide a reportable measurement of an organization's compliance with established cybersecurity practices. Example items tracked by the scorecard include maintaining appropriate versions of software, ensuring proper use of PKIs, adhering to secure network architectures, and addressing any identified vulnerabilities.

5.4.8. Vulnerability and Cyber Incident Management

DTSA requires Vulnerability and Cyber Incident Management support across its IT Enterprise. This includes plans, processes, and procedures remediation and mitigation of for vulnerabilities, incidents, and events as well as the application of patches and secure configurations. The contractor shall:

5.4.8.1. DTSA requires Vulnerability and Cyber Incident Management support across its IT Enterprise. This includes plans, processes, and procedures remediation and mitigation of for vulnerabilities, incidents, and events as well as the application of patches and secure configurations. The contractor shall:

5.4.8.2. Develop and maintain a comprehensive Cyber Incident Response Plan for the DTSA IT Enterprise. The plan must address processes and procedures all forms of cyber incident and event as well as data spillages and issues related to user behavior. Additionally, it must document roles and responsibilities (e.g. RACI) and integrate interfaces with service providers and reporting agencies including but not limited to Pentagon Computer Emergency Response Team (PENTCERT), C5ISR CSSP, or other agencies external to DTSA as required.

5.4.8.3. Respond to all cyber incidents, events, and spills as required in the DTSA Cyber Incident Response Plan. Additionally, provide dynamic status information for any active incident as well as preliminary and final reports for each incident. This include After Action Reports and Analysis as recording and integration lessons learned.

5.4.8.4. Providing monthly metrics on quantity, type, and performance on incident response processes.

5.4.8.5. Develop a Cyber Hardening SOP for planning, testing, and applying DISA Security Technical Implementation Guide (STIG) requirements, Secure Requirements Guides (SRG), and vendor patches as well as applying vendor and provider hardening guidance across the DTSA IT enterprise. This also includes, but is not limited to, U.S. Cyber Commands Information Assurance Vulnerability Alerts (IAVAs), and bulletins, Orders (e.g., OpOrds, WarnOrds, TaskOrds) and Directives.

5.4.8.6. Implement approved Cyber Hardening SOP providing metrics and details on performance and compliance at weekly, biweekly, and monthly intervals.

5.4.8.7. Develop Cyber Operations SOPs for security tools appliances and capabilities in use within the DTSA IT Enterprise to levels and standards required by DoD (USCYBERCOM, JFHQ-DoDIN, DISA, JSP, etc.) policy, regulation, and guidance. This includes but is not limited to Host-Based Security Server (HBSS), Assured Compliance Assessment Solution (ACAS), Security Content Automation Protocol (SCAP) Compliance Checker (SCC), PKI, and anti-virus software. These standards and tools can change any time as required by governing federal agencies.

5.4.8.8. Implement approved Cyber Operating SOPs providing metrics and details on performance and compliance at weekly, biweekly, and monthly intervals.

5.4.8.9. Provide Vulnerability Reports using mandated DoD and or COR/GTM tools (e.g. ACAS). Reports shall include data form all mandated scans/reports in mandated tool guidance.

5.4.8.10. Provide Endpoint Security Reports using mandated DoD and or COR/GTM tools (e.g. HBSS/ESS). Reports shall include data form all mandated scans/reports in mandated tool guidance.

5.4.9. Asset Management

DTSA desires assets and property management support for DTSA IT Enterprise assets. This support is typical of a Property Custodian within DISA, DLA, and DTSA constructs. The contractor shall: Develop an Asset Management SOP that facilitates and enables maintain 100% accountability of all DTSA IT equipment (including hardware, software, and data) as required by the risk management framework and other DoD, DISA, DLA, and DTSA requirements.

5.4.9.1. Implement approved Asset Management SOP.

5.4.9.2. Support and conduct common practices for ordering assets, tracking orders and assets, tagging hardware assets, disposal, transfers and other lifecycle roles.

5.4.9.3. Where permissible, acquire accounts and access to property management systems and support DTSA Property Custodian tasking.

## 5.5. Task Area 5: Information, Knowledge Management, and Training

### 5.5.1. Documentation

DTSA requires development, maintenance, and curation of documentation related to its IT Enterprise and associated business. The contractor shall:

5.5.1.1. Develop and maintain a record management plan for DTSA IT Enterprise and its related business. The plan must comply with regulations set forth by the DoD, Washington Headquarters Service (WHS), and the National Archives Records Administration (NARA) and still allow for ease of use. Additionally, adherence and assistance with adherence to the plan once approved is expected.

5.5.1.2. Develop and maintain generalized and system development lifecycle documentation for the DTSA IT Enterprise. Generalized documentation includes but is not limited to on-line help, quick guides, user guides, standard operating documents, maintenance documents, training manuals, installation guides, configuration control board (CCB) minutes, and build documentation for all hardware, software, and service components. System development life cycle documentation can include, but is not limited to, requirements, design, development, test, implementation and O&M artifacts as well as various network, system, application and data diagrams.

5.5.1.3. Deliver all documentation in electric format, understanding that, in certain instances, paper documentation may be required. All documentation, including all files and documentation related to this PWS, shall be stored in an electronic/digital repository (e.g.: share drive, portal, wiki).

### 5.5.2. Training and User Assistance

DTSA requires a comprehensive set of training material and support for DTSA IT Enterprise users. The contractor shall:

5.5.2.1. Develop and provide training, user assistance, and desk guides for all DTSA internal users on user IT solutions and capabilities. This includes using services offered by JSP (or successor service providers), DISA, and other service.

5.5.2.2. Develop and provide training on DTSA IT Enterprise mission applications. This formal instruction shall include user guide development, distribution and enhancements, as well as hands-on familiarization of common IT and DTSA IT Enterprise mission applications. Periodic refresher training may additionally be provided as necessary, and as required by DTSA management.

5.5.2.3. Develop and provide ad hoc training to individuals and small groups on COTS and GOTS features and capabilities, as appropriate.

5.5.3. Knowledge Management

DTSA expects a robust set of knowledge management and web services to facilitate information across its broad range of customers and partners. This includes Web and Social Media Support, internal and external portals, and compliance elements of those capabilities. The contractor shall:

5.5.3.1. Develop and maintain a Social Media SOP that addresses stewardship and management of social media presence including processes for posting to various social media in compliance with various with DoD and DTSA policies as well as socials media accounts and identify management procedures. The SOP shall provide architecture definition and guiding principles, governance structures and processes, and development tools and methodologies and maintain currency with industry-best practices and government standards, guidelines and regulations for developing, deploying, and maintaining web sites. Compliance with DoD, cyber, OPSEC, and OSD Public Affairs is expected in the SOP as well.

5.5.3.2. In compliance with the Social Media SOP, provide web and social media design, development and maintenance support. This includes managing DTSA websites, content development, portals, their underlying databases, and posting to social media sites (e.g.: Twitter, YouTube, etc.).

5.5.3.3. Develop and maintain a Knowledge Management SOP and Strategy for a DTSA portal. The SOP shall facilitate processes and procedures to systemically link and/or reproduce relevant information from diverse sources to form a single and virtual knowledge repository (e.g. SharePoint portal). It must also implement best business practices to ensure that information and knowledge is timely, accurate, and relevant. Additionally, it must provide a framework for content owners and managers to develop their own pages and content.

5.5.3.4. Develop and maintain a Knowledge Management SOP and Strategy for a DTSA portal. The SOP shall facilitate processes and procedures to systemically link and/or reproduce relevant information from diverse sources to form a single and virtual knowledge repository (e.g. SharePoint portal). It must govern collection and synthesis end user requirements as the basis to design, develop and deploy and implement best business practices to ensure that information and knowledge is timely, accurate, and relevant. Additionally, it must provide a framework for content owners and managers to develop their own pages and content.

5.5.3.5. Establish leadership dashboards and standard displays to convey relevant information, facilitate a shared understanding of key information amongst decision makers, and provide an enterprise context for decisions.

5.5.3.6. Assist development of content owner and mangers in the development of Knowledge Management pages and sites. This includes collection and synthesis of end user requirements as the basis to design, develop and deploy web sites, Intranets and portals as well as assistance with content posting. All requests shall be captured, tracked, and dispositioned via the change request processes.

5.5.3.7. Ensure that all websites and web applications meet the standards regulated by Section 508 of the Rehabilitation Act of 1973; available at: http://www.section508.gov.

5.5.4. Process Management and Improvement

DTSA requires expert process management and improvement capability to support end-to-end process framework documentation and continuous process improvement of its IT and business processes. The contractor shall:

5.5.4.1. Develop a plan to iteratively review and document DTSA IT and business processes and hone apply various techniques to improve organizational performance and efficiency. This includes examining organizational and interagency goals, objectives, structures/hierarchies, systems and roles for the purpose of evolving the long-term, full-scale integration activities for the DTSA IT Enterprise. Plan must also include templates/formats for process artifacts.

5.5.4.2. Conduct and host process mapping and documentation functions of DTSA IT and business processes throughout the agency to enable automation efforts and improve support overall across the agency. Process artifacts will be stored and curated in a centralized location determined by the government.

5.5.4.3. Use a range of process mapping techniques including, but not limited to, value stream mapping, Lean/Six Sigma, DMAIC, PDCA, and BPM to guide DTSA through regular improvement.

## 5.6. Task Area 6: Enhanced IT Capabilities (Optional Tasks)

### 5.6.1. Cross-Domain Solution

DTSA seeks an Automated Cross-Domain Solution (CDS) to facilitate transfer between NIPRNET and SIPRNET IT Enterprise systems. Tasks in the PWS section are broke up by the "direction" of the transfer, but in practice may be combined for efficiency or to take advantage of unique opportunities that benefit DTSA. The contractor shall:

5.6.1.1. Research and gather business and IT requirements, processes, procedures and data types eligible for inclusion in an Automated Cross-Domain Solution (CDS) for both low to high and high to low transfers.

5.6.1.2. Develop acquisition, management, deployment, and other plans to implement a CDS for low-to-high data transfers between Secret and unclassified domains within the DTSA IT enterprise with preference for DoD-enterprise wide solutions as well as cloud solutions. Plans must include CDS authorization and sustainment needs.

5.6.1.3. Implement approved plans for a CDS capable of low-to-high data transfers between Secret and unclassified domains.

5.6.1.4. Develop acquisition, management, deployment, and other plans to implement a CDS for high-to-low data transfers between Secret and unclassified domains within the DTSA IT enterprise with preference for DoD-enterprise wide solutions as well as cloud solutions. Plans must include CDS authorization and sustainment needs.

5.6.1.5. Implement approved plans for a CDS capable of high-to-low data transfers between Secret and unclassified domains.

### 5.6.2. Surge Application Development, Enhancement, and Customization

DTSA seeks Surge Application Development, Enhancement, and Customization support. This includes dedicated resources to focus on development, enhancement, updated, and/or customization of DTSA IT Enterprise Applications for a specific and time-bound iteration of development beyond capacity built into the capacity of the PWS. Work done will comply and synchronize with all other portions of the PWS to ensure a homogenous integration with the rest of the DTSA IT Enterprise.

5.6.2.1. Develop and deploy a specific and time-bound iteration of enhancement or customization of the DTSA IT Enterprise in accordance with approved government development processes and as approved by requisite change management processes.

5.6.2.2. Integrate development activities and outputs into the DTSA IT Enterprise and its baselines.

# PART 6

# APPLICABLE PUBLICATIONS

## 6. APPLICABLE PUBLICATIONS

The Contractor must abide by all applicable regulations, publications, manuals, and local policies and procedures. The contractor will be required to remain knowledgeable and apply any updated/replacement versions of these publications.

As policy frequently changes in the IT and technology domain, the contractor will be expected to adapt and assimilate new editions of publications into their execution of the PWS.

Table 6:A. Applicable Publications

| # | Document Number | Title |
|---|---|---|
| 1 | DoDD 5105.72 | DoD Directive – Defense Technology Security Administration (DTSA) |
| 2 | 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 |
| 3 | DoDM 5200.02 | DoD Manual – Procedures for the DoD Personnel Security Program dtd 3 Apr 17 |
| 4 | DoDD 5205.02E | DoD Directive – Operations Security (OPSEC) Program dtd 20 Jun 12 with Change 2 dtd 20 Aug 20 |
| 5 | DoDM 5205.02 | DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08 with Change 1 dtd 26 Apr 18 |
| 6 | DoDI 5200.48 | DoD Instruction – Controlled Unclassified Information (CUI) dtd 6 Mar 20 |
| 7 | DoDD 8140.01 | DoD Directive – Cyberspace Workforce Management dtd 05 Oct 20 |
| 8 | DoDI 8500.01 | DoD Instruction – Cybersecurity dtd 14 Mar 14 with Change 1 dtd 07 Oct 19 |
| 9 | 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 |
| 10 | DoD 8570.01-M | DoD Manual – Information Assurance Workforce Improvement Program dtd 19 Dec 05 with Change 3 dtd 24 Jan 12 and Change 4 dtd 10 Nov 15 (and subsequent replacement) |
| 11 | Privacy Act of 1974 | United States federal law, Pub.L. 93–579, 88 Stat. 1896, dtd December 31, 1974, 5 U.S.C. § 552a |
| 12 | CJSCI 6510.01F | Information Assurance (IA) and Support to Computer Network Defense (CND) |
| 13 | CJCSM 6510.01B | Cyber Incident Handling Program |
| 14 | 32 CFR Part 117 | NISPOM Rule – Previously as DoD Policy DOD 5220.22-M |
| 15 | CNSSI 4009 | Committee on National Security Systems Instruction Number 4009, “Committee on National Security Systems (CNSS) Glossary,” April 6, 2015 |
| 16 | CNSSI 1253 | Security Categorization and Control Selection for National Security System |
| 17 | DoDD 5105.72 | DoD Directive – Defense Technology Security Administration (DTSA) |
| 18 | Public Law 111-292 | Telework Enhancement Act of 2010, 2021 Guide to Telework and Remote Work in the Federal Government |
| 19 | NIST SP 800-30, Rev 1 | Guide for Conducting Risk Assessments |
| 20 | NIST SP 800-34, Rev 1 | Contingency Planning Guide for Federal Information Systems |
| 21 | NIST SP 800-37, Rev 2 | Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy |
| 22 | NIST SP 800-53, Rev 3 | Security and Privacy Controls for Information Systems and Organizations |
| 23 | NIST SP 800-53A, Rev 5 | Assessing Security and Privacy Controls in Information Systems and Organizations |
| 24 | | Department of Defense Software Modernization Strategy<br>DoD Enterprise DevSecOps Strategy Guide dtd 19 Oct 2021 |
| 25 | | DoD Enterprise DevSecOps Fundamentals dtd 19 Oct 2021 |
| 26 | | DevSecOps Playbook dtd 19 Oct 2021 |
| 27 | | DevSecOps Fundamentals Guidebook: DevSecOps Tools & Activities dtd 19 Oct 2021 |
| 28 | | DoD Data Strategy dtd 30 SEPT 2020 |

# PART 7

# ATTACHMENT/TECHNICAL EXHIBIT LISTING

## 7. ATTACHMENT/TECHNICAL EXHIBIT LIST

Exhibit 1 – Performance Requirements Summary

Exhibit 2 – Deliverables Schedule

Exhibit 3 – Personnel and Labor Category Qualifications

Exhibit 4 – Estimated Workload and Environment Data

Exhibit 5 – Estimated ODC

Exhibit 6 – Table of Contents

## 7.1. Exhibit 1 – Performance Requirements Summary

The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 1 | 5.2.1. | The contract shall perform tasks in section 5.2.1. Program Management Planning | Program Management Plan | Plan contains required information and is delivered on time. Revisions that occur are minor and are resolved in a satisfactory manner. Utilizes PMI/ITIL or other IT/Project management body of knowledge | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 2 | 5.2.1. | The contract shall perform tasks in section 5.2.1. Program Management Planning | Staff/Resource Management Plan | Includes<br>Contractor Certification List<br>[A list of all contractor employees, certification and training that is planned and/or received, and expiration date].<br>Staffing Plan<br>Utilizes PMI/ITIL or other IT/Project management body of knowledge | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 3 | 5.2.1. | The contract shall perform tasks in section 5.2.1. Program Management Planning | Project-specific PMPs | Plan contains required information and is delivered on time. Revisions that occur are minor and are resolved in a satisfactory manner. Utilizes PMI/ITIL or other IT/Project management body of knowledge | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 4 | 5.2.1. | The contract shall perform tasks in section 5.2.1. Program Management Planning | Program Management Plan and/or Service Management Plans | Plan contains required information and is delivered on time. Revisions that occur are minor and are resolved in a satisfactory manner. Utilizes PMI/ITIL or other IT/Project management body of knowledge | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 5 | 5.2.2. | The contract shall perform tasks in section 5.2.2. Status Reporting | Monthly Information Technology Program Report | Brief contains key elements required in PWS. Contains excerpts from existing reports. Reports contain required information and are delivered on time at least 90% of the time. Revisions that occur are minor and are resolved in a satisfactory manner. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 6 | 5.2.2. | The contract shall perform tasks in section 5.2.2. Status Reporting | Daily Application and Capability Health Report SOP | SOP addresses what to measure and how to measure them. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 7 | 5.2.2. | The contract shall perform tasks in section 5.2.2. Status Reporting | Daily Application and Capability Health Reports | Reports comply with SOP. Reports contain required information and are delivered on time at least 90% of the time. Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 8 | 5.2.2. | The contract shall perform tasks in section 5.2.2. Status Reporting | Monthly Network Availability Performance Metrics Report SOP | SOP addresses what to measure and how to measure them. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 9 | 5.2.2. | The contract shall perform tasks in section 5.2.2. Status Reporting | Monthly Network Availability Performance Metrics Reports | Reports comply with SOP.<br>Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 10 | 5.2.3. | The contract shall perform tasks in section 5.2.3. Change Management Support | CCB Charter for each I/CCB | Plan implements DTSA CIO Change Management Vision.<br>Charters utilize best practices in PMI/ITIL or other IT/Project management body of knowledge.<br>Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 11 | 5.2.3. | The contract shall perform tasks in section 5.2.3. Change Management Support | Change Management Plan for the agency-level and each CCB hosted by DTSA | Plan implements DTSA CIO Change Management Vision.<br>Charters utilize best practices in PMI/ITIL or other IT/Project management body of knowledge.<br>Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 12 | 5.2.3. | The contract shall perform tasks in section 5.2.3. Change Management Support | CCB briefing materials<br>Executed CCB Meetings<br>Meeting minutes, votes, and other records | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Complies with charters and CM Plans. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 13 | 5.2.3. | The contract shall perform tasks in section 5.2.3. Change Management Support | Complexity Framework Documentation | Provides framework for estimating complexity, cost, and risk as well as development and implementation time.<br>Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 14 | 5.2.3. | The contract shall perform tasks in section 5.2.3. Change Management Support | Investment and Development analysis | Complies with Complexity Framework<br>Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 15 | 5.2.3. | The contract shall perform tasks in section 5.2.3. Change Management Support | Active list of all CRs, their impacts, scope and schedule (estimated and actual). | List includes all details about all CRs<br>Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Complies with charters and CM Plans. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 16 | 5.2.4. | The contract shall perform tasks in section 5.2.4. Configuration Management | Configuration Management Plan (CMP) | Plan implements DTSA CIO Change Management Vision.<br>Charters utilize best practices in PMI/ITIL or other IT/Project management body of knowledge.<br>Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 17 | 5.2.4. | The contract shall perform tasks in section 5.2.4. Configuration Management | Active list of Cis | List includes all details about all CRs<br>Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Complies with charters and CM Plans. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 18 | 5.2.5. | The contract shall perform tasks in section 5.2.5. Program Management Support | PMIS | Utilize best practices in PMI/ITIL or other IT/Project management body of knowledge.<br>Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 19 | 5.2.5. | The contract shall perform tasks in section 5.2.5. Program Management Support | PMIS Training Material | Utilize best practices in PMI/ITIL or other IT/Project management body of knowledge.<br>Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 20 | 5.2.6. | The contract shall perform tasks in section 5.2.6. Metrics and Evaluation | Evaluation Plan | Provides measurement approach for each element in PWS<br>Provides enough metrics to assess and inform on application and capability health.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 21 | 5.2.6. | The contract shall perform tasks in section 5.2.6. Metrics and Evaluation | Compliance with Evaluation Plan | Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 22 | 5.2.7. | The contract shall perform tasks in section 5.2.7. Contract Transition | Schedule and coordinate and execute a Kick-Off Meeting Contract Kick-Off Agenda and Briefing Slides | Materials contain required information and are delivered on time. Revisions that occur are minor and are resolved in a satisfactory manner. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 23 | 5.2.7. | The contract shall perform tasks in section 5.2.7. Contract Transition | Kick Off Contract Transition Plan | Materials contain required information and are delivered on time. Revisions that occur are minor and are resolved in a satisfactory manner. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 24 | 5.2.7. | The contract shall perform tasks in section 5.2.7. Contract Transition | End-of-Contract Transition Plan | Materials contain required information and are delivered on time. Revisions that occur are minor and are resolved in a satisfactory manner. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 25 | 5.3.1. | The contract shall perform tasks in section 5.3.1. Managed Services | Managed Service SOP | SOP ensures (not an exhaustive list):<br>-Implemented a USG approved SOP for the acquisition of IT managed services.<br>-All Acquisitions are in accordance with provisions of FAR 51.1.<br>-Contractor will document and track all IT managed service acquisitions.<br>SOPs contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 26 | 5.3.1. | The contract shall perform tasks in section 5.3.1. Managed Services | Support the USG for acquisition of managed services | Implemented a USG approved SOP for the acquisition of IT managed services.<br>All Acquisitions are in accordance with provisions of FAR 51.1.<br>Contractor will document and track all IT managed service acquisitions.<br>SOPs contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 27 | 5.3.2. | The contract shall perform tasks in section 5.3.2. Acquisition | IT Acquisition SOP | SOP includes all aspects required for acquisition of commodity IT software and equipment.<br>SOP includes reporting requirements and compliance requirements. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 28 | 5.3.2. | The contract shall perform tasks in section 5.3.2. Acquisition | Manage software license agreements. | All agreements are documented, tracked, maintained, and updated/renewed, with COR/GTM approval, with zero loss in services.<br>Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 29 | 5.3.2. | The contract shall perform tasks in section 5.3.2. Acquisition | Support the DTSA in the acquisition of hardware, software, services, and related capabilities. | All acquisitions are in accordance with provisions of FAR 51.1.<br>Contractor documents and tracks all IT equipment acquisitions.<br>Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 30 | 5.3.2. | The contract shall perform tasks in section 5.3.2. Acquisition | Support the DTSA in the acquisition of hardware, software, services, and related capabilities.<br>A minimum of three hardware quotes for each hardware item that is being purchased. | Implemented a USG approved standard process for the acquisition of Hardware, software, services, and related capabilities.<br>All acquisitions are in accordance with provisions of FAR 51.1.<br>Contractor documents and tracks all hardware, software, services, and related capability acquisitions.<br>Quotes contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 31 | 5.3.3. | The contract shall perform tasks in section 5.3.3. Market Research and Prototyping | Provide recommendations for a prototype product. | Prototypes are efficiently utilized to test new technologies, reduce program risk, and save life cycle costs. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 32 | 5.3.3. | The contract shall perform tasks in section 5.3.3. Market Research and Prototyping | Provide recommendations to resolve IT problems with commercial off-the-shelf (COTS) solutions that are National Information Assurance Partnership (NIAP)-approved as well as on DISA's Approved Products List (APL) | Recommendations are sound and support the DTSA IT Enterprise mission.<br>Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 33 | 5.4.1. | The contract shall perform tasks in section 5.4.1. Enterprise IT Policy and Planning | IT strategy, roadmaps, polices, plans, standards, processes, procedures and other documents and artifacts | Complies with requirements in PWS.<br>Recommendations are sound and support the DTSA IT Enterprise mission.<br>Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 34 | 5.4.1. | The contract shall perform tasks in section 5.4.1. Enterprise IT Policy and Planning | Data Strategy and Implementation Plan | Complies with requirements in PWS.<br>Recommendations are sound and support the DTSA IT Enterprise mission.<br>Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 35 | 5.4.1. | The contract shall perform tasks in section 5.4.1. Enterprise IT Policy and Planning | Application Modernization Plan | Plan addresses all DTSA Application environment needs and provides complete plan to implement modernization, with increments of plan compartmentalized to be change requests. | Deliverable and Work Product Review and Evaluation |
| 36 | 5.4.1. | The contract shall perform tasks in section 5.4.1. Enterprise IT Policy and Planning | Cloud Services Delivery Strategy | Strategy identifies each element of the DTSA IT Enterprise and shows how each can iterate cloud native technologies. | Deliverable and Work Product Review and Evaluation |
| 37 | 5.4.1. | The contract shall perform tasks in section 5.4.1. Enterprise IT Policy and Planning | Technology upgrade artifacts | Recommendations are sound and support the DTSA IT Enterprise mission.<br>Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Deliverable and Work Product Review and Evaluation |
| 38 | 5.4.2. | The contract shall perform tasks in section 5.4.2. Requirements Analysis | End-User Requirements Report. | Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Deliverable and Work Product Review and Evaluation |
| 39 | 5.4.3. | The contract shall perform tasks in section 5.4.3. Application Development, Enhancement, and Customization | Development SOP | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>SOP includes all elements in PWS. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 40 | 5.4.3. | The contract shall perform tasks in section 5.4.3. Application Development, Enhancement, and Customization | System Development Life Cycle Documentation<br>RMF Artifacts | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Consistent with Development SOP | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 41 | 5.4.4. | The contract shall perform tasks in section 5.4.4. IT Operations and Support | IT Operations SOP | SOP addresses all DTSA enterprise and non-enterprise applications, enterprise consolidated non-production and production hosting environments, servers, services, storage systems networks (physical or virtual) and systems.<br>SOP addresses and adheres to all applicable DoD policies (e.g.: STIGS, SRGs, etc) and industry best practices.<br>SOP shall also include reporting and metrics for IT Operations Health.<br>SOP must also drive the following (this is not an all inclusive list):<br>Efficiently manage DTSA IT Enterprise domain controller resources.<br>Ensure old accounts are terminated, and new accounts are created within 24 hours of request.<br>Ensure user account information is documented and stored utilizing proper PII procedures, as necessary".<br>Ensure that all application, messaging, collaboration environments are operational at least 90% of the time to all authorized end users and customers.<br>Manage the resources and activities for DTSA IT Enterprise domain controllers, permissions, user account information, activation, deactivation, authentication, and enforce DoD security policies within the Windows domain environment.<br>Install, configure, maintain, and upgrade Windows member servers<br>Implement server notification warnings | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 42 | 5.4.4. | The contract shall perform tasks in section 5.4.4. IT Operations and Support | Managed DTSA IT Enterprise | Managed DTSA IT Enterprise managed in accordance with SOP. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 43 | 5.4.4. | The contract shall perform tasks in section 5.4.4. IT Operations and Support | Data Dictionaries<br>Structures and Architectures<br>Entity Relationship Diagrams<br>Guidance Documents for Data Standards | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Support the development, maintenance, modification and retirement of all data dictionaries, data structures and architectures, entity- relationship diagrams, and guidance documents. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 44 | 5.4.4. | The contract shall perform tasks in section 5.4.4. IT Operations and Support | Provide installation and configuration of new or existing IT equipment. | IT equipment is adequately installed/configured, and in working condition 99% of the time.<br>New installations/configurations are performed in a timely manner to meet mission needs.<br>Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 45 | 5.4.4. | The contract shall perform tasks in section 5.4.4. IT Operations and Support | Application Operations Report SOP | SOP addresses the following:<br>DTSA IT Enterprise applications and associated IT resources are operational and properly functioning 95% of the time.<br>Connectivity between DTSA and mission partners are established with traffic data rates adequate to meet the mission need 95% of the time.<br>Outages are resolved efficiently with minimal down time. All network modifications and configuration changes are properly documented.<br>Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | 0 |
| 46 | 5.4.4. | The contract shall perform tasks in section 5.4.4. IT Operations and Support | Maintain all DTSA IT Enterprise applications and associated IT resources (e.g.: servers).<br>Provide a control point to resolve and implement LAN configuration issues and equipment hookups; analyze, isolate and coordinate corrective action for communications -related problems; and the configuration of communications equipment in support of these environments. | DTSA IT Enterprise applications and associated IT resources are operational and properly functioning 95% of the time.<br>Connectivity between DTSA and mission partners are established with traffic data rates adequate to meet the mission need 95% of the time.<br>Outages are resolved efficiently with minimal down time. All network modifications and configuration changes are properly documented.<br>Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 47 | 5.4.4. | The contract shall perform tasks in section 5.4.4. IT Operations and Support | Storage Optimization Report SOP | SOP addresses the following:<br>All historical, current, and future storage capacity planning requirements are recorded.<br>Additional storage capability added, as required, with COR/GTM approval.<br>Zero Data loss under nominal conditions; No more than 24 hours of data loss in a COOP/recovery scenario.<br>Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 48 | 5.4.4. | The contract shall perform tasks in section 5.4.4. IT Operations and Support | Determine the optimum storage capacity for increased storage and retrieval requirements.<br>Report on storage utilization (used/free) space. | All historical, current, and future storage capacity planning requirements are recorded.<br>Additional storage capability added, as required, with COR/GTM approval.<br>Zero Data loss under nominal conditions; No more than 24 hours of data loss in a COOP/recovery scenario.<br>Reports contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 49 | 5.4.5. | The contract shall perform tasks in section 5.4.5. Business Continuity Support | IT Continuity of Operations Plan (COOP)<br>Disaster Recovery Plan (DRP) | Plans contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Restoration capabilities include:<br>Ensure DTSA IT Enterprise and Applications, messaging, collaboration environments are operational at least 90% of the time to all authorized end users and customers.<br>In a COOP scenario: COOP site should be operational within 24 hours following a COOP activation notification from the Director or DTSA.<br>No more than 24 hours of data loss from the time the primary system becomes unavailable.<br>Plans contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 50 | 5.4.5. | The contract shall perform tasks in section 5.4.5. Business Continuity Support | COOP/DRP Tests and results. | Test meets scope approved by COR/GTM<br>Tests result in successful service restoration. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 51 | 5.4.5. | The contract shall perform tasks in section 5.4.5. Business Continuity Support | IT Continuity of Operations Plan (COOP) and inputs. | Staff Certificates and credentials are documented and maintained in a single document and stored electronically in a common file/folder.<br>Plans contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 52 | 5.4.5. | The contract shall perform tasks in section 5.4.5. Business Continuity Support | Disaster Recovery Plan (DRP) and inputs | Plans contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 53 | 5.4.6. | The contract shall perform tasks in section 5.4.6. Service Desk | Service Desk SOPs | SOPs contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Drives resolution of greater than 90% of all critical (Mission Essential Function or VIP operations) customer support requests within two business hours; and resolve greater than 80% of all non-critical customer support requests within eight business hours.<br>SOPs contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 54 | 5.4.6. | The contract shall perform tasks in section 5.4.6. Service Desk | Certificate, token, and authenticators | DTSA IT Enterprise applications accessible via PKI infrastructure 99% of the time.<br>PKI materials contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 55 | 5.4.6. | The contract shall perform tasks in section 5.4.6. Service Desk | Completed Server Certificate Form(s) | DTSA IT Enterprise applications accessible via PKI infrastructure 99% of the time.<br>PKI materials contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 56 | 5.4.6. | The contract shall perform tasks in section 5.4.6. Service Desk | User Access Report | User Access Report shows quantities of accounts in total as well as those added, deleted, and or changed for each resource with the DTSA IT Enterprise.<br>User Access Report shows metrics for Certificate, token, and authenticators issued or revoked.<br>Delivered on time at least 90% of the time | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 57 | 5.4.6. | The contract shall perform tasks in section 5.4.6. Service Desk | Monthly Trouble Ticket Activities Report on Service Desk performance | Resolve greater than 90% of all critical (Mission Essential Function or VIP operations) customer support requests within two business hours; and resolve greater than 80% of all non-critical customer support requests within eight business hours. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 58 | 5.4.7. | The contract shall perform tasks in section 5.4.7. Cybersecurity and Compliance | RMF Process SOP | SOP addresses all requirements for DoD RMF policy, instructions, and manuals.<br>Deviations are presented to and approved by COR/GTM in writing. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 59 | 5.4.7. | The contract shall perform tasks in section 5.4.7. Cybersecurity and Compliance | Reports from RMF Process and Workflow system (e.g. eMASS/ERS) | DTSA applications are properly authorized 99% of the time.<br>POAMs contain comprehensive remediation information and are delivered on time at least 95% of the time. Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 60 | 5.4.7. | The contract shall perform tasks in section 5.4.7. Cybersecurity and Compliance | Compliant execution of RMF Process Guide | Record vulnerabilities, risks, and mitigations.<br>POAMs vulnerabilities are resolved within the prescribed timeframe captured in the POAM. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 61 | 5.4.7. | The contract shall perform tasks in section 5.4.7. Cybersecurity and Compliance | Record vulnerabilities, risks, and mitigations | DTSA applications are properly authorized 99% of the time.<br>POAMs contain comprehensive remediation information and are delivered on time at least 95% of the time. Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 62 | 5.4.7. | The contract shall perform tasks in section 5.4.7. Cybersecurity and Compliance | Support and apply POA&M remediation techniques throughout the Applications, systems, and enclaves lifecycle. | POAMs vulnerabilities are resolved within the prescribed timeframe captured in the POA&M. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 63 | 5.4.7. | The contract shall perform tasks in section 5.4.7. Cybersecurity and Compliance | Support all internal and external IT related inspections and evaluations. | Participates in inspection/evaluation preparations (self- inspections, pre- briefs, peer reviews) 99% of the time.<br>Resolves known issues prior to inspection 95% of the time.<br>Adequately corrects all findings, via proper procedures, in a timely manner 99% of the time.<br>Participates in inspection/evaluation follow-up activities 99% of the time. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 64 | 5.4.7. | The contract shall perform tasks in section 5.4.7. Cybersecurity and Compliance | Inspection Readiness Reports | Reports track all details of CCRI, CCORI, and CSSP Inspections.<br>Reports are updated at least monthly.<br>Data is accurate 95%.<br>Data in reports shows passing inspection scores. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 65 | 5.4.7. | The contract shall perform tasks in section 5.4.7. Cybersecurity and Compliance | Support all internal and external IT related inspections and evaluations | Reports track all details of CCRI, CCORI, and CSSP Inspections.<br>Reports are updated at least monthly.<br>Data is accurate 95%.<br>Data in reports shows passing inspection scores. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 66 | 5.4.7. | The contract shall perform tasks in section 5.4.7. Cybersecurity and Compliance | Implement, operate, and maintain Scorecard system of record (e.g. EMASS/ERS) | FISMA/SECDEF/Cyber scorecards' data is submitted for USG review by established due dates 99.9% of the time | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 67 | 5.4.8. | The contract shall perform tasks in section 5.4.8. Vulnerability and Cyber Incident Management | Cyber Incident Response Plan | Compliance with DoD Instructions and policy as well as National Institute of Standards and Technology Special Publications | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 68 | 5.4.8. | The contract shall perform tasks in section 5.4.8. Vulnerability and Cyber Incident Management | Incident Response Report | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Reports are consistent with IRP Requirements | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 69 | 5.4.8. | The contract shall perform tasks in section 5.4.8. Vulnerability and Cyber Incident Management | Cyber Incident Response Metrics Report | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Reports are consistent with IRP Requirements. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 70 | 5.4.8. | The contract shall perform tasks in section 5.4.8. Vulnerability and Cyber Incident Management | Cyber Hardening SOP | Compliance with DoD Instructions and policy as well as National Institute of Standards and Technology Special Publications<br>SOPs contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 71 | 5.4.8. | The contract shall perform tasks in section 5.4.8. Vulnerability and Cyber Incident Management | Metrics on Cyber Hardening | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Reports are consistent with Cyber Hardening SOP. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 72 | 5.4.8. | The contract shall perform tasks in section 5.4.8. Vulnerability and Cyber Incident Management | Cyber Operating SOP | Compliance with DoD Instructions and policy as well as National Institute of Standards and Technology Special Publications<br>SOPs contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 73 | 5.4.8. | The contract shall perform tasks in section 5.4.8. Vulnerability and Cyber Incident Management | Meet Threshold Compliancy Percentages<br>Implement, operate and maintain Assured Compliance Assessment Solution (ACAS) and/or successor tool.<br>Evaluate compliance with Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG), implement patches of SPAN to mitigate U.S. Cyber Commands Information Assurance Vulnerability Alerts (IAVAs), and bulletins, as well as Orders (e.g., OpOrds, WarnOrds, TaskOrds) and Directives | All security and related monitoring and scanning solutions are properly configured more than 95% of the time.<br>All devices scanned weekly 95% of the time.<br>Daily scans are Devices patched in accordance with<br>DISA standards<br>(Critical/High<br>vulnerabilities w/in 7<br>required unless<br>altered by the USG.<br>30 days) | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 74 | 5.4.8. | The contract shall perform tasks in section 5.4.8. Vulnerability and Cyber Incident Management | Implement, operate and maintain Host- Based Security Server (HBSS) and/or successor tool.<br>Meet Threshold Compliancy Percentages | All security and related monitoring and scanning solutions are properly configured more than 95% of the time.<br>All devices scanned weekly 95% of the time.<br>Daily scans are Devices patched in accordance with DISA standards (Critical/High vulnerabilities w/in 7 required unless altered by the USG. )<br>Point product deployment meets the following:<br>HBSS Point Product \|\| Threshold Compliancy Percentage \|\| Objective Compliancy Percentage<br>McAfee Agent \|\| 95% \|\| 99%<br>Virus Scan \|\| 95% \|\| 99%<br>DAT version Virus Scan \|\| 95% \|\| 99%<br>Host Intrusion Prevention \|\| 95% \|\| 99%<br>Data Loss Prevention \|\| 95% \|\| 99%<br>USAF ACCM \|\| 95% \|\| 99%<br>Policy Auditor Agent \|\| 95% \|\| 99% | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 75 | 5.4.9. | The contract shall perform tasks in section 5.4.9. Asset Management | Asset Management SOP | Complies with DoD, DISA, DLA, and DTSA requirements.<br>Enables asset tracking to individual users. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 76 | 5.4.9. | The contract shall perform tasks in section 5.4.9. Asset Management | Completed Asset Management Forms (e.g. DD1150) | Forms are completed timely | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 77 | 5.5.1. | The contract shall perform tasks in section 5.5.1. Documentation | Record Management Plan | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 78 | 5.5.1. | The contract shall perform tasks in section 5.5.1. Documentation | On-line help, quick guides, user guides, standard operating documents, maintenance documents, training manuals, installation guides, and build documentation for all hardware and software components<br>System development lifecycle documentation.<br>Network, system, application and data diagrams. | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Documentation is updated within 1 month of a life cycle change | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 79 | 5.5.2. | The contract shall perform tasks in section 5.5.2. Training and User Assistance | User IT solutions and capabilities Training | Develop, maintain, and implement User IT solutions and capabilities Training<br>Training materials contain required information and are delivered on time at least 90% of the time. Revisions that occur are minor and are resolved in a satisfactory manner | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 80 | 5.5.2. | The contract shall perform tasks in section 5.5.2. Training and User Assistance | DTSA IT Enterprise and Applications Training | Develop, maintain, and implement DTSA IT Enterprise and Applications Training Sessions (Basic, Intermediate, advanced, and Custom/specialized courses based on mission need).<br>Training may be located in DTSA training room or other customer facility.<br>Training materials contain required information and are delivered on time at least 90% of the time. Revisions that occur are minor and are resolved in a satisfactory manner | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 81 | 5.5.3. | The contract shall perform tasks in section 5.5.3. Knowledge Management | Social Media SOP | Addresses stewardship and management of social media presence including processes for posting to various social media in compliance with various with DoD and DTSA policies as well as socials media accounts and identify management procedures.<br>Provides architecture definition and guiding principles, governance structures and processes, and development tools and methodologies and maintain currency with industry-best practices and government standards, guidelines and regulations for developing, deploying, and maintaining web sites.<br>Compliance with DoD, cyber, OPSEC, and OSD Public Affairs is expected in the SOP as well. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 82 | 5.5.3. | The contract shall perform tasks in section 5.5.3. Knowledge Management | DTSA Web Portal Plan and Portal itself | Plan addresses all internal DTSA communication needs and requirements, including allowing for updates for different business areas within DTSA.<br>Contractor will be expected to conduct requirements gathering to build out portal.<br>Actual portal implementation matches approved government plan.<br>Portal is easily maintainable via DTSA government and contractor users' business areas. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 83 | 5.5.3. | The contract shall perform tasks in section 5.5.3. Knowledge Management | Knowledge Management SOP and Strategy | Facilitate processes and procedures to systemically link and/or reproduce relevant information from diverse sources to form a single and virtual knowledge repository (e.g. SharePoint portal).<br>Governs collection and synthesis end user requirements as the basis to design, develop and deploy and implement best business practices to ensure that information and knowledge is timely, accurate, and relevant.<br>Provide a framework for content owners and managers to develop their own pages and content. | Process Monitoring<br>Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 84 | 5.5.3. | The contract shall perform tasks in section 5.5.3. Knowledge Management | Section 508 of the Rehabilitation Act of 1973 Compliance on all web sites and applications. | Compliance with Section 508 Accessibility Technical Standards:<br>• 1194.21 - Software Applications and Operating Systems<br>• 1194.22 - Web Based Intranet and Internet Information and Applications<br>• 1194.41 - Information, Documentation and Support<br>Compliance with Section 508 Accessibility Functional Performance Criteria:<br>• 1 1194.31 - Functional Performance Criteria | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 85 | 5.5.4. | The contract shall perform tasks in section 5.5.4. Process Management and Improvement | Process Management and Improvement Plan | Deliverables contain required information and are delivered on time at least 90% of the time. Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 86 | 5.5.4. | The contract shall perform tasks in section 5.5.4. Process Management and Improvement | Process Maps and artifacts | Deliverables contain required information and are delivered on time at least 90% of the time. Revisions that occur are minor and are resolved in a satisfactory manner.<br>Deliverables accurately describe business processes<br>Format is consistent with Process Management and Improvement Plan | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

| # | PWS | Performance Objective | Standard | Performance Threshold | Method of Surveillance |
|---|---|---|---|---|---|
| 87 | 5.5.4. | The contract shall perform tasks in section 5.5.4. Process Management and Improvement | Documented business processes featuring workflows and SOPs | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Deliverables accurately describe business processes<br>Format is consistent with Process Management and Improvement Plan | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 88 | 5.6.1. | The contract shall perform tasks in section 5.6.1. Cross-Domain Solution | Cross-Domain Solution business and IT requirements | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Requirements capture include all DTSA needs | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 89 | 5.6.1. | The contract shall perform tasks in section 5.6.1. Cross-Domain Solution | Low-to-High CDS Plans | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 90 | 5.6.1. | The contract shall perform tasks in section 5.6.1. Cross-Domain Solution | High-to-Low CDS Plans | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner. | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |
| 91 | 5.6.2. | The contract shall perform tasks in section 5.6.2. Surge Application Development, Enhancement, and Customization | Enhancement or Customization of the DTSA IT Enterprise | Deliverables contain required information and are delivered on time at least 90% of the time.<br>Revisions that occur are minor and are resolved in a satisfactory manner.<br>Enhancement or Customization complies with Change Request | Comprehensive Inspections<br>Deliverable and Work Product Review and Evaluation |

## 7.2. Exhibit 2 – Deliverables Schedule

| # | PWS | Deliverable | Frequency | Deadline/Due Date | Medium/Format | Submit To |
|---|---|---|---|---|---|---|
| 1 | 5.2.1. | Program Management Plan | Once<br>Updated as required | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution* |
| 2 | 5.2.1. | Staff/Resource Management Plan | Once<br>Updated as required<br>Quarterly | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution* |
| 3 | 5.2.1. | Project-specific PMPs | Once<br>Updated as required | Within 10 days of Project assignment. | Microsoft Office/Office365 Suite Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution* |
| 4 | 5.2.1. | Program Management Plan and/or Service Management Plans | Once<br>Updated as required | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution* |
| 5 | 5.2.2. | Monthly Information Technology Program Report | Monthly | Present report by second Monday of each Month<br>Report Due preceding Thursday at COB | Microsoft Office PowerPoint | Standard Distribution* |
| 6 | 5.2.2. | Daily Application and Capability Health Report SOP | Once<br>Updated as required | Draft due NLT 15 days from contract award.<br>Final due no later than 5 days after USG provide their comments.<br>Updates due 3 days after request by COR/GTM | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 7 | 5.2.2. | Daily Application and Capability Health Reports | Daily (Weekdays only) | NLT 0800 daily | Email | Standard Distribution* |
| 8 | 5.2.2. | Monthly Network Availability Performance Metrics Report SOP | Once<br>Updated as required | Draft due NLT 15 days from contract award.<br>Final due no later than 5 days after USG provide their comments.<br>Updates due 3 days after request by COR/GTM | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 9 | 5.2.2. | Monthly Network Availability Performance Metrics Reports | Monthly | 10th day of each month | Microsoft Office/Office365 Suite Formats | Standard Distribution* |

| # | PWS | Deliverable | Frequency | Deadline/Due Date | Medium/Format | Submit To |
|---|---|---|---|---|---|---|
| 10 | 5.2.3. | CCB Charter for each I/CCB | Once<br>Updated as required | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite<br>Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution* |
| 11 | 5.2.3. | Change Management Plan for the agency-level and each CCB hosted by DTSA | Once<br>Updated as required | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite<br>Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution* |
| 12 | 5.2.3. | CCB briefing materials<br>Executed CCB Meetings<br>Meeting minutes, votes, and other records | Approximately 30-40 meetings over the course of a 12-month period | No later than one week prior to the specific meeting(s).<br>Draft slides due to USG and user community NLT 3 days prior to meeting(s).<br>Final document(s) due NLT the date/time of the meeting(s). | Microsoft Office/Office365 Suite<br>Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution*<br>CCB Members |
| 13 | 5.2.3. | Complexity Framework Documentation | Once<br>Updated as required | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite<br>Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution*<br>CCB Members |
| 14 | 5.2.3. | Investment and Development analysis | As required by CCB | As required by CCB | Microsoft Office/Office365 Suite<br>Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution*<br>CCB Members |
| 15 | 5.2.3. | Active list of all CRs, their impacts, scope and schedule (estimated and actual). | Continuously | Updated list of all CRs due NLT the 5 business days after CCB. | Microsoft Office/Office365 Suite<br>Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge<br>As Defined by the CCB | Standard Distribution*<br>CCB Members |
| 16 | 5.2.4. | Configuration Management Plan (CMP) | Once<br>Updated as required | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite<br>Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge<br>As Defined by the CCB | Standard Distribution*<br>CCB Members |
| 17 | 5.2.4. | Active list of Cis | Continuously | Continuously | Microsoft Office/Office365 Suite<br>Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge<br>As Defined by the CCB | Standard Distribution*<br>CCB Members |
| 18 | 5.2.5. | PMIS | Once<br>Updated weekly or as required | Established NLT 150 days from contract award. | Microsoft Office/Office365 Suite<br>Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution* |

| # | PWS | Deliverable | Frequency | Deadline/Due Date | Medium/Format | Submit To |
|---|---|---|---|---|---|---|
| 19 | 5.2.5. | PMIS Training Material | Once<br>Updated as required | Draft due NLT 15 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution* |
| 20 | 5.2.6. | Evaluation Plan | Once<br>Updated as required | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution* |
| 21 | 5.2.6. | Metrics and Evaluation Report | Monthly<br>Out-of-cycle As required | Due every last Friday of month<br>Out-of-cycle As required | Microsoft Office/Office365 Suite Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution* |
| 22 | 5.2.7. | Contract Kick-Off Agenda and Briefing Slides | Once | Read ahead material due one (1) business day prior to meeting<br>Briefing slides/handout s due by the day/time of meeting | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 23 | 5.2.7. | Kick Off Contract Transition Plan | Once | Read ahead material due one (1) business day prior to meeting<br>Briefing slides/handout s due by the day/time of meeting | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 24 | 5.2.7. | Contract (End) Transition Plan | Once<br>Updated as required | NLT 90 Days from Period-of-Performance End | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 25 | 5.3.1. | Managed Service SOP | Once<br>Updated as required | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution* |
| 26 | 5.3.1. | Managed Services | Continuously | Continuously | Microsoft Office/Office365 Suite Formats<br>Formats native to managed service | Standard Distribution* |
| 27 | 5.3.2. | IT Acquisition SOP | Once<br>Updated as required | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats with structure/format adapted from PMI/ITIL or other IT/Project management body of knowledge | Standard Distribution* |
| 28 | 5.3.2. | Software License Report | Monthly | First issuance 30 days after contract award.<br>10th day of each month | Microsoft Office/Office365 Suite Formats | Standard Distribution* |

| # | PWS | Deliverable | Frequency | Deadline/Due Date | Medium/Format | Submit To |
|---|---|---|---|---|---|---|
| 29 | 5.3.2. | IT Acquisition Report | Monthly. Updated when a license is acquired, renewed, modified or eliminated. Updated NLT 3 business days prior to any cyber inspection. | 10th day of each month | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 30 | 5.3.2. | Quotes on hardware, software, services, and related capabilities. | As required | NLT 10 days from request | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 31 | 5.3.3. | Market research and/or prototyping information Analysis | As required by COR/GTM | As required by COR/GTM | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 32 | 5.3.3. | COTS products recommendations as required by the USG | As required by COR/GTM | As required by COR/GTM | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 33 | 5.4.1. | IT strategy, roadmaps, polices, plans, standards, processes, procedures and other documents and artifacts | As required | As required by COR/GTM | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 34 | 5.4.1. | Data Strategy and Implementation Plan | Once<br>Updated as required | 60 days after contract award | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 35 | 5.4.1. | Application Modernization Plan | Once<br>Updated as required | NLT 60 days after contract award | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 36 | 5.4.1. | Cloud Services Delivery Strategy | Once<br>Updated as required | NLT 60 days after contract award | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 37 | 5.4.1. | Technology upgrade artifacts including on-line help, quick guides, user guides, standard operating documents, maintenance documents, training manuals, installation guides, and build documentation for all hardware and software components. | One time per document | 5 business days prior to user acceptance testing | Microsoft Office/Office365 Suite Formats | Standard Distribution*<br>Loaded as change Request in appropriate CCB |

| # | PWS | Deliverable | Frequency | Deadline/Due Date | Medium/Format | Submit To |
|---|---|---|---|---|---|---|
| 38 | 5.4.2. | End-User Requirements Report.<br>[Identifies who requested the requirement, if the requirement was approved/denied, justification for approval or denial, and the date the requirement was implemented or denied] | One time per change request | NLT 5 days after receiving the change request | Microsoft Office/Office365 Suite Formats | Standard Distribution*<br>CCB Members<br>Change request review meetings |
| 39 | 5.4.3. | Development SOP | Once<br>Updated as required | Draft due NLT 15 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 40 | 5.4.3. | System Development Life Cycle Documentation<br>RMF Artifacts | Updated at the conclusion of each enhancement, and as required thereafter. | As agreed by COR/GTM | Microsoft Office/Office365 Suite Formats<br>Application (e.g.: eMASS) or Process specific formats | Standard Distribution* |
| 41 | 5.4.3. | Mission application development methodology/process(es) | Annually<br>Updated as Required | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 42 | 5.4.4. | IT Operations SOP | Once<br>Updated as required | Draft due NLT 15 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 43 | 5.4.4. | Managed DTSA IT Enterprise | Daily | Continuous | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 44 | 5.4.4. | Data Dictionaries<br>Structures and Architectures<br>Entity Relationship Diagrams<br>Guidance Documents for Data Standards | At least once following an change | Initial/Original due NLT than 15 Days after Contract Award<br>10 business days following change to structure or architecture | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 45 | 5.4.4. | Equipment Installation Report | As required by COR/GTM | NLT 5 Days after installation Requests | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 46 | 5.4.4. | Application Operations Report SOP | Once<br>Updated as required | Draft due NLT 15 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |

| # | PWS | Deliverable | Frequency | Deadline/Due Date | Medium/Format | Submit To |
|---|---|---|---|---|---|---|
| 47 | 5.4.4. | Application Operations Report | Monthly<br>Updated NLT 3 business days prior to any inspection | 30 days after contract award<br>10th day of each month thereafter | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 48 | 5.4.4. | Storage Optimization Report SOP | Once<br>Updated as required | Draft due NLT 15 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 49 | 5.4.4. | Storage Optimization Report | Monthly<br>Updated NLT 3 business days prior to any inspection | 30 days after contract award<br>10th day of each month thereafter | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 50 | 5.4.5. | IT Continuity of Operations Plan (COOP) Disaster Recovery Plan (DRP) | Updated Quarterly<br>Updated within 15 days of change in COOP capability. | Draft due NLT 90 days from contract award.<br>Final due 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 51 | 5.4.5. | COOP/DRP Tests and results. | Tests Conducted Quarterly or when capabilities change. | First test conducted 180 days after contract award and ever 180 days there after with COR/GTM approval.<br>Test Report due NLT 5 days after test. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 52 | 5.4.5. | IT Continuity of Operations Plan (COOP) and inputs. | Updated Quarterly<br>Updated within 15 days of change in COOP capability. | Draft due NLT 90 days from contract award.<br>Final due 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 53 | 5.4.5. | Disaster Recovery Plan (DRP) and inputs | Updated Quarterly<br>Updated within 15 days of change in COOP capability. | Draft due NLT 90 days from contract award.<br>Final due 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 54 | 5.4.6. | Service Desk SOPs | Annually<br>Updated as Required | 45 days after contract award<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 55 | 5.4.6. | Certificate, token, and authenticators | As requested | NLT than 5 days from request | USG provided format | Standard Distribution* |
| 56 | 5.4.6. | Completed Server Certificate Form(s) | When a server certificate requires renewal | NLT 28 days before the server certification expiration date | USG provided format | Standard Distribution* |
| 57 | 5.4.6. | User Access Report | Monthly | Initial report due 7 days after contract award<br>The 10th day of each month, thereafter. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 58 | 5.4.6. | Trouble Ticket Activities Report on Service Desk performance | Monthly | 20th day of each month | Microsoft Office/Office365 Suite Formats | Standard Distribution* |

| # | PWS | Deliverable | Frequency | Deadline/Due Date | Medium/Format | Submit To |
|---|---|---|---|---|---|---|
| 59 | 5.4.7. | RMF Process SOP | Annually<br>Updated as Required | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 60 | 5.4.7. | Reports from RMF Process and Workflow system (e.g. eMASS/ERS) | Monthly | First report due NLT 60 days from contract award.<br>15th day of each month thereafter | Microsoft Office/Office365 Suite Formats<br>Native Reports from RMF Process and Workflow system | Standard Distribution* |
| 61 | 5.4.7. | RMF POAMs for each DTSA IT Enterprise Application by authorization boundary | Monthly<br>According to POAM dates | As required by USG for the upcoming month AND NLT 3 business days prior to cyber inspections. | Microsoft Office/Office365 Suite Formats<br>RMF Process and Workflow system (e.g. eMASS/ERS). | Standard Distribution*<br>RMF Process and Workflow system (e.g. eMASS/ERS). |
| 62 | 5.4.7. | Updated RMF POAMs for each DTSA IT Enterprise Application by authorization boundary | Monthly<br>According to POAM dates | Resolved according to the due dates in the POAM. | Microsoft Office/Office365 Suite Formats<br>RMF Process and Workflow system (e.g. eMASS/ERS). | Standard Distribution*<br>RMF Process and Workflow system (e.g. eMASS/ERS). |
| 63 | 5.4.7. | Inspection Readiness Reports | Monthly | First report due NLT 60 days from contract award.<br>15th day of each month thereafter | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 64 | 5.4.7. | Completed Cyber Inspection Action Items | As determined by the Inspector(s) | As determined by the Inspector(s) | As determined by the Inspector(s)<br>Microsoft Office/Office365 Suite Formats | Standard Distribution*<br>As determined by the Inspector(s) |
| 65 | 5.4.7. | FISMA/SECDEF/Cyber scorecard reporting documentation for U.S. Government submission. | Monthly | NLT 2 business days prior to the end of the month. AND NLT 3 business days prior to any cyber Inspections.<br>As required by USG for the upcoming month AND NLT 3 business days prior to cyber inspections. | Microsoft Office/Office365 Suite Formats<br>Scorecard system of record (e.g. EMASS/ERS) | Standard Distribution*<br>Scorecard system of record (e.g. EMASS/ERS) |
| 66 | 5.4.8. | Cyber Incident Response Plan | Annually<br>Updated as Required<br>Updated after Lessons Learned from Incident/Event/etc | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 67 | 5.4.8. | Incident Response Report | As required | Preliminary due within 2 hours of incident/event notification.<br>Final Report with after action and lessons learned due 3 days after closure. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 68 | 5.4.8. | Cyber Incident Response Metrics Report | Monthly | First report due NLT 30 days from contract award.<br>15th day of each month thereafter | Microsoft Office/Office365 Suite Formats | Standard Distribution* |

| # | PWS | Deliverable | Frequency | Deadline/Due Date | Medium/Format | Submit To |
|---|---|---|---|---|---|---|
| 69 | 5.4.8. | Cyber Hardening SOP | Annually<br>Update Quarterly | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 70 | 5.4.8. | Metrics on Cyber Hardening | Monthly | First report due NLT 30 days from contract award.<br>15th day of each month thereafter | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 71 | 5.4.8. | Cyber Operating SOP | Annually<br>Update Quarterly | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 72 | 5.4.8. | Vulnerability Reports | Daily | Daily | Mandated Tool-Native formats<br>Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 73 | 5.4.8. | Endpoint Security Reports | Daily | Daily | Mandated Tool-Native formats<br>Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 74 | 5.4.9. | Asset Management SOP | Once<br>Updated as required | Draft SOP due NLT 30 days from contract award.<br>Final SOP due 15 days after USG provide their comments | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 75 | 5.4.9. | Completed Asset Management Forms (e.g. DD1150) | As required | NLT 5 days after request | Microsoft Office/Office365 Suite Formats<br>PDF Forms | Standard Distribution*<br>POCs on forms |
| 76 | 5.5.1. | Record Management Plan | Once<br>Updated as required | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 77 | 5.5.1. | On-line help, quick guides, user guides, standard operating documents, maintenance documents, training manuals, installation guides, and build documentation for all hardware and software components.<br>System development life cycle documentation.<br>Network, system, application and data diagrams. | One time per document | 5 business days prior to user acceptance testing<br>As required by the development cycle | Microsoft Office/Office365 Suite Formats<br>Directly into applications as applicable. | Standard Distribution* |

| # | PWS | Deliverable | Frequency | Deadline/Due Date | Medium/Format | Submit To |
|---|---|---|---|---|---|---|
| 78 | 5.5.2. | Internal personnel training on user IT solutions and capabilities<br>COR/GTM will provide required items that must be addressed] | As required | As required | Microsoft Office/Office365 Suite Formats<br>Classroom/Virtual Formats | Standard Distribution*<br>Distribution dependent on training audience |
| 79 | 5.5.2. | Internal and external personnel training on DTSA IT Enterprise and Applications<br>COR/GTM will provide required items that must be addressed] | As required | As training commitments arise | Microsoft Office/Office365 Suite Formats<br>Classroom/Virtual Formats | Standard Distribution*<br>Distribution dependent on training audience |
| 80 | 5.5.3. | Social Media SOP | Once<br>Updated as required | Draft due NLT 90 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 81 | 5.5.3. | DTSA Web Portal | Updated Dynamically | Draft plan due NLT 30 days from contract award.<br>Final Plan due 15 days after USG provide their comments.<br>Portal completed according to plan 30 days after final plan acceptance | Microsoft Sharepoint site/pages | Plan to Standard Distribution*<br>Portal itself on USG Sharepoint |
| 82 | 5.5.3. | Knowledge Management SOP and Strategy | Once<br>Updated as required | Draft due NLT 30 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 83 | 5.5.3. | Section 508 Compliance Report | With every change to websites and web applications. | Prior to change | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 84 | 5.5.4. | Process Management and Improvement Plan | Once<br>Updated as required | Draft due NLT 90 days from contract award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 85 | 5.5.4. | Process Maps and artifacts | As required by COR/GTM | NLT 5 days after function<br>As required by COR/GTM | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 86 | 5.5.4. | Documented business processes featuring workflows and SOPs | As required by COR/GTM | As required by COR/GTM | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 87 | 5.6.1. | Cross-Domain Solution business and IT requirements | Once<br>Updated as required | Draft due NLT 30 days from contract/task award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |

| # | PWS | Deliverable | Frequency | Deadline/Due Date | Medium/Format | Submit To |
|---|---|---|---|---|---|---|
| 88 | 5.6.1. | Low-to-High CDS Plans | Once<br>Updated as required | Draft due NLT 90 days from contract/task award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 89 | 5.6.1. | High-to-Low CDS Plans | Once<br>Updated as required | Draft due NLT 90 days from contract/task award.<br>Final due no later than 15 days after USG provide their comments. | Microsoft Office/Office365 Suite Formats | Standard Distribution* |
| 90 | 5.6.2. | Enhancement or Customization of the DTSA IT Enterprise | Once per CLIN Award | By end of Timebound increment | Microsoft Office/Office365 Suite Formats for documentation Enhancement or Customization of the DTSA IT Enterprise | Standard Distribution* |

## 7.3. Exhibit 3 – Personnel and Labor Category Qualifications

The following table establishes certification and personnel security clearance requirements for contractor employees. Certification requirements are in accordance with DoD 8570.01-M and DFARS 252.239.7001. Key personnel requirements may exceed that which is listed in the table below.

Table 7:A. Labor Category Qualifications

| # | Labor Category | Certification Level | Personnel Security Clearance | Investigation |
|---|---|---|---|---|
| 1 | Business Process Reengineering Specialist - Level II | IAT Level I | SECRET | T3 |
| 2 | Cloud Solutions Architect | IAT Level II | SECRET | T3 |
| 3 | Computer Security System Specialist – Level II | IAT Level II | TOP SECRET | T3 |
| 4 | Computer Security System Specialist – Level III | IAT Level II | TOP SECRET w/ SCI Eligibility | T5 |
| 5 | Data Scientist | IAT Level II | SECRET | T3 |
| 6 | Database Administrator | IAT Level II | SECRET | T3 |
| 7 | Database Specialist – Level II | IAT Level II | SECRET | T3 |
| 8 | Information Systems Training Specialist | IAT Level I | SECRET | T3 |
| 9 | Knowledge Engineer | IAT Level I | SECRET | T3 |
| 10 | Project Management Analyst | IAT Level I | SECRET | T3 |
| 11 | Project Manager - Level III | IAT Level I | TOP SECRET | T5 |
| 12 | System Administrator - Level I | IAT Level II | SECRET | T3 |
| 13 | System Administrator - Level II | IAT Level II | SECRET | T3 |
| 14 | System Administrator - Level III | IAT Level II | SECRET | T3 |
| 15 | System Engineer - Level II | IAT Level II | SECRET | T3 |
| 16 | System Programmer | IAT Level I | SECRET | T3 |
| 17 | Tech Writer | IAT Level I | SECRET | T3 |

Additionally the following tasks from Part 5: Specific Tasks require personnel security clearance requirements for contractor employees above SECRET. Again, key personnel requirements may exceed that which is listed in the table below.

Table 7:B. Task Qualifications

| # | Task | Personnel Security Clearance | Investigation |
|---|---|---|---|
| 1 | 5.4.7. Cybersecurity and Compliance | TOP SECRET | T5 |
| 2 | 5.4.8. Vulnerability and Cyber Incident Management | TOP SECRET | T5 |

## 7.4. Exhibit 4 – Estimated Workload and Environment Data

Table 7:C. Estimated Hours per Year

| Estimated Hours per Year | 1,992 |
|---|---|

Table 7:D. Estimated Labor

| # | Labor Category | FTE | Hours (Per Year) |
|---|---|---|---|
| 1 | Business Process Reengineering Specialist - Level II | 2 | 3,984 |
| 2 | Cloud Solutions Architect | 1 | 1,992 |
| 3 | Computer Security System Specialist – Level II | 3 | 5,976 |
| 4 | Computer Security System Specialist – Level III | 1 | 1,992 |
| 5 | Data Scientist | 1 | 1,992 |
| 6 | Database Administrator | 1 | 1,992 |
| 7 | Database Specialist – Level II | 2 | 3,984 |
| 8 | Information Systems Training Specialist | 3 | 5,976 |
| 9 | Knowledge Engineer | 2 | 3,984 |
| 10 | Project Management Analyst | 1 | 1,992 |
| 11 | Project Manager - Level III | 1 | 1,992 |
| 12 | System Administrator - Level I | 2 | 3,984 |
| 13 | System Administrator - Level II | 1 | 1,992 |
| 14 | System Administrator - Level III | 1 | 1,992 |
| 15 | System Engineer - Level II | 4 | 7,968 |
| 16 | System Programmer | 6 | 11,952 |
| 17 | Tech Writer | 1 | 1,992 |

Table 7:E. DTSA Applications

| # | Application | Environment | Architecture in FY22 | Desired Architecture |
|---|---|---|---|---|
| 1 | USXPORTS | SIRPNET On-Prem | Client-Server | Web Application/Microservices |
| 2 | USX Lite | IL5 Azure | Web Application | Web Application/Microservices |
| 3 | NDPS | SIRPNET On-Prem | Web Application | Web Application/Microservices |
| 4 | FVS-DoD | SIRPNET On-Prem | Client-Server | Web Application/Microservices |
| 5 | FVS-E | IL5 Azure | Client-Server | Web Application/Microservices |
| 6 | FVS-CM | IL5 Azure | Client-Server | Web Application/Microservices |
| 7 | DPARS | IL5 Azure | Web Application | Web Application/Microservices |
| 8 | SPACE Link | IL5 Azure | Web Application | Web Application/Microservices |
| 9 | Elisa | IL2 Azure | Web Application | Web Application/Microservices |
| 10 | DTSA Public website | IL2 Azure | Web Application | Web Application |

## 7.5. Exhibit 5 – Estimated ODC Items

Table 7:F. Estimated ODC Items

| # | Item | Quantity |
|---|---|---|
| 1 | F5 License Subscription | 1 |
| 2 | Citrix XenDesktop License Subscription | 1 |
| 3 | Adobe Creative Cloud for Teams-License Subscription | 2 |
| 4 | Rapid Spell Desktop.NET Annual Maintenance | 2 |
| 5 | Citrix Netscaler Subscription | 1 |
| 6 | Redgate SQL Bundle Professional Support & Upgrade | 1 |
| 7 | Microsoft Terminal Services Clients | 200 |
| 8 | Microsoft SQL Server 2019 Enterprise (1 Clusters) | 4 |
| 9 | Entrust SSL Certificates | 1 |
| 10 | Service Now | 1 |
| 11 | UiPath Software | 1 |

## 7.6. Exhibit 6 – Table of Contents