**PERFORMANCE WORK STATEMENT (PWS)**

**as of *[DD-MMM-YYYY]***

|  |  |
| --- | --- |
| **Contractor Name:** | *[Insert Company Name]* |
| **GSA Schedule Contract Number** | *[Insert Contract Number]* |
| **GSA BPA Number** | *[TBD]* |

*[Fill-in guidance is presented in* ***RED ITALIC*** *with brackets borders.* ***REMEMBER*** *to delete all italicized text, contained within brackets herein when completing your PWS.* *It is shown here for instructional/informational purposes only and must not remain part of the final document/proposal submitted.]*

# Background

The Department of Defense (DoD) requires an integrated enterprise cloud service offering (CSO) that provides common communication, collaboration, and productivity capabilities that are mission-effective, efficient, more widely accessible, and facilitate DoD operations worldwide. The Defense Information Systems Agency (DISA), in support of the DoD Deputy Secretary of Defense’s direction to accelerate the DoD’s adoption of cloud

computing technology, plans to acquire and implement a seamlessly integrated, enterprise CSO as a replacement for disparate DoD legacy enterprise information technology (IT) services, such as voice, video, collaboration, email, content management, records management, and productivity suite.

# Objectives

DEOS will support the Department’s vision to move towards an integrated/interoperable communication,

collaboration, and productivity service, by facilitating trusted information sharing between Combatant

Commands, Services and Agencies (CC/S/As), and through the consolidation of multiple DoD enterprise services into a single environment. In addition, DEOS will unify and modernize legacy DISA IT enterprise services such as DoD Enterprise email (DEE), DoD Enterprise Portal Service (DEPS), Defense Collaboration Services (DCS), and other DoD-wide legacy capabilities.

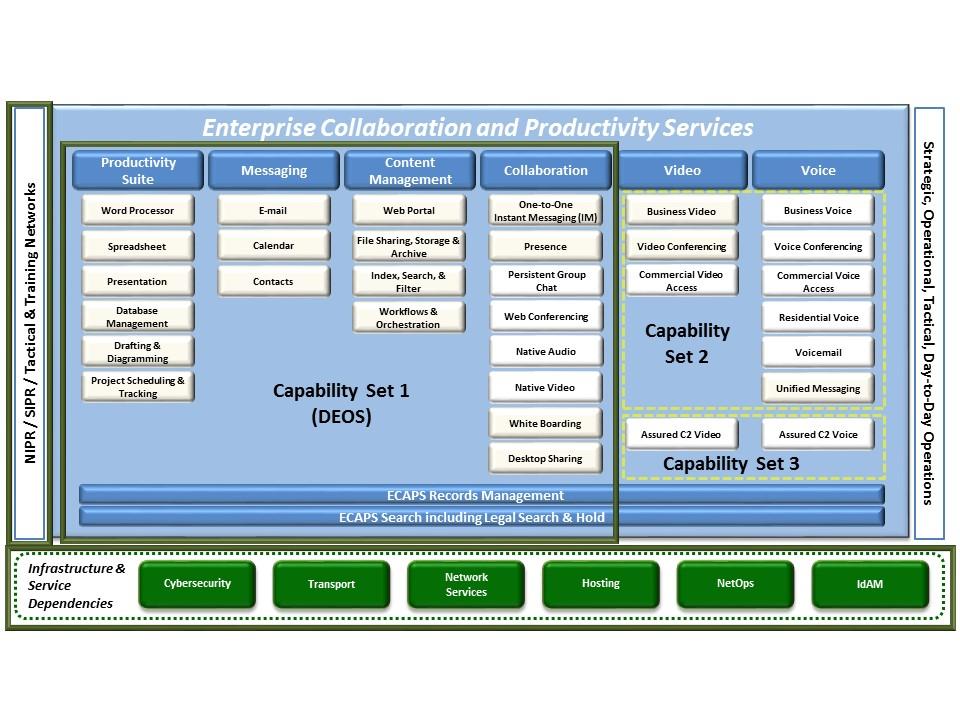
The DEOS CSO will be acquired by DISA using an unrestricted, competitively awarded, single-award Firm-Fixed Price (FFP) Blanket Purchase Agreement (BPA) with a contractor who will provide a widely used/widely available, and non-developmental and fully integrated collaboration solution. The BPAperiod of performance will be a 5-year base ordering period and two 2 year option periods and one 1 year option period.. The BPAalso will include the 6-month extension of services authorized by FAR 52.217-8. The 10-year period of performance will provide the Department with the flexibility to transition users based on user demand, migration schedules, and legacy contracts or service end-of-life terms

# Scope

The DEOS CSO may scale to an anticipated 3.15 million DoD consumers, and over 4 million directory objects, which includes supporting DoD CC/S/As across many locations to include local base/post/camp/station (B/P/C/S), deployed and afloat organizations. DEOS is intended to be deployed on the Sensitive but Unclassified Internet Protocol (SBU IP) Data Network, also known as NIPRNet, and the Secret Internet Protocol (IP) Data, also known as SIPRNet, to include Denied, Disconnected, Intermittent, and Limited Bandwidth (D-DIL)

environments.

The capabilities within the scope of the DEOS service are highlighted in Figure 1. The green boxes highlight the key DoD supporting infrastructure, services, and major integration points that will reside primarily on-premises as part of the Government’s responsibility. The Cloud Service Provider (CSP) will be responsible for ensuring interoperability and integration with these major service support functions and integration points. Additional requirements are outlined in section 6, and section 7 of the Functional Requirements Document (FRD) Attachment A.



**Figure 1 – DEOS Service Requirements**

The Government requires a multifaceted implementation and deployment approach for United States territories and possessions and locations outside of the United States territories and possessions for NIPRNet, SIPRNet, and D-DIL environments.

For NIPRNet and SIPRNet implementations in United States territories and possessions, the Government expects to leverage DoD approved commercially hosted facilities to meet the DEOS requirements. However, due to DoD data sovereignty requirements, the contractor must implement their NIPRNet and SIPRNet CSO within DoD data centers (e.g., Stuttgart, Wiesbaden, Capodichino) for locations outside of the United States territories and possessions.

For locations outside of the United States territories and possessions, the contractor must provide a standalone environment within a DoD data center. The solution must be self-contained and must include the required infrastructure, hardware, software, and auxiliary components required to implement, management, and maintain the CSO environment within the DoD data center. The Government expects the contractor to describe the details of their solution to include physical requirements (e.g., number of distributed DoD data centers), heating, ventilation, air condition (HVAC), per-rack power (e.g., single phase, 3-phase, amperage, voltage, etc.), floor space (e.g., rack and total square footage), bandwidth (in total Mbps/Gbps), physical security/separation, physical access, remote management, and networking (e.g., IP addressing, subnets, routing) requirements.

# Performance Requirements

The contractor shall propose performance tasks that fully adhere to the requirements of the solicitation and the DEOS FRD (Attachment A) so that DEOS is available to end users. The contractor will perform all necessary activities as well as provide the required documentation association to achieve and maintain the necessary DEOS Authorization to Operate (ATO) decisions as a national security system on the DoDIN, utilizing the Performance Work Statement (PWS) format (Attachment C) provided as part of this solicitation.

## Task 1 – NIPRNet Environment

The contractor shall deliver a CSO that enables collaboration across the DoD enterprise. The NIPRNet CSO shall include System Wide, Core Services (i.e., email, IM/chat, web conferencing, native audio, native video, content management, and productivity suite), and DoD Information Network (DoDIN) Protection requirements in

accordance with (IAW) the FRD sections 1, 2, and 3 having a network category of “Both” or “NIPR”.

Furthermore, the contractor shall be required to interface the CSO to the core integration points identified in the FRD section 6. Lastly, the contractor shall adhere to the performance objectives identified in the FRD section 8, and shall be required to perform testing activities/events (i.e., integration, acceptance, operational) IAW the FRD section 9, to verify the proper interoperability between the CSO and core integration points (FRD section 6).

#### Subtask 1 – United States Territories and Possessions

Provide a geographically dispersed ***off-premises*** CSO within a DoD private/community hybrid cloud that meets Impact Level 5 requirements IAW the DoD CCSRG and the FRD.

#### Subtask 2 – Locations outside of the United States Territories and Possessions

Provide a geographically dispersed DoD private/community Cloud Service Offering (CSO) that is deployed in an DoD facility using an ***on-premises*** deployment model that meets Impact Level 5 in accordance with the DoD CC SRG and FRD.

#### Deliverables

The Government shall require the following documents as key deliverables for this task and sub-tasks. All deliverables listed below correspond with the key program milestones, activates, and deliverables listed in Attachment D. Any additional deliverables (i.e. not indicated below or in attachment D) maybe required by the Government based on the proposed technical/management approach and will be included at task order execution.

*[The contractor shall propose any additional deliverables based upon their technical and management approach that collectively provide sufficient evidence of satisfactory performance of activities required for this task and sub-tasks as applicable. Any additional deliverables included within the table below should also be included in key program milestone, activities, and deliverables list Attachment D]*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Deliverable Name** | | **Format** | **Due Date (Notional)** | **Distribution** | **Classification** | **Frequency** |
| Architecture, DoDAF Artifacts/Diagrams (AV, OV, SV, StdV, CV) \* | | Government Determined Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| System Design Document \*\* | | Government Determined Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Interfaces, Ports & Protocols Baseline \*\* | | Contractor Determined Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Service Support Functions and Integration Plan \* | | Contractor Determined / Government Approved Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Performance Monitoring Strategy \* | | Contractor Determined / Government Approved Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Security Architecture Analysis \* | | Contractor Determined / Government Approved Format | 30 days after Task Order Execution | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Communication Plan \* | | Contractor Determined / Government Approved Format | 30 days after Task Order Execution | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Migration Schedule \* | | Contractor Determined Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Service Management Plan \*\* (To Address: Access Management,  Event Management,  Incident Management,  Request Fulfillment,  Storefront Integration,  Service Desk Support  Network Operations (NetOps)  Service Desk Integration (i.e., GSD and/or Mission Partner) OSS/JMN and Out of Band (OOB) management) | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Preliminary Design Review | Distribution D | **CUI** | One Time; updated as required |
| Change Management Plan \* | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Tenancy Review | Distribution D | **CUI** | One Time; updated as required |
| Incident Response Plan and Procedures \* | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Tenancy Review | Distribution D | **CUI** | One Time; updated as required |
| Service Desk Strategy \* | | Contractor Determined Format | 30 days after Acceptance of Tenancy Review | Distribution D | **CUI** | One Time; updated as required |
| System Administrator Configuration Guides for NIPR \* | | Contractor Determined / Government Approved Format | 15 days after Acceptance of Production Readiness Review | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Impact Assessment Report \* | | Government Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Implementation Status Report \* | | Contractor Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Implemented Cybersecurity Controls Checklist \* | | Contractor Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Cybersecurity Assessment Report \* | | Government Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Selected Security Control Assessment \* | | Government Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Issue Resolution/Remediation Report \* | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Risk Acceptance Recommendation \* | | Contractor Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Continuous monitoring strategy/plan \*\*/† | | Government Determined Format | 30 days after Acceptance of Provisional Authorization | Distribution D | **CUI** | One Time; updated as required |
| System Security Plan (SSP) \*\* | | Government Determined Format | 30 days after Acceptance of Provisional Authorization | Distribution D | **CUI** | One Time; updated as required |
| Directory Replication Plan \*\* | | Contractor Determined Format | 45 days after Acceptance of Provisional Authorization | Distribution D | **CUI** | One Time; updated as required |
| OCSP/CRL Integration Plan \* | | Contractor Determined Format | 45 days after Acceptance of Provisional Authorization | Distribution D | **CUI** | One Time; updated as required |
| Provisioning / Authentication Assessment Documentation \*/† | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Yearly; as required |
| Privacy Impact Assessment \*/† | | Government Determined Format | 15 days after IdAM Integration | Distribution D | **CUI** | Yearly; as required |
| Privacy Threshold Analysis \*/† | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Yearly; as required |
| Residual Risk Statement \*/† | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Yearly; as required |
| Vulnerability Assessment \*/† | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Monthly; as required |
| Business Impact Analysis \* | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Monthly; as required |
| Contingency Plan \* | | Contractor Determined / Government Approved Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Monthly; as required |
| Continuous Monitoring Test Plan \*/† | | Contractor Determined / Government Approved Format | 30 days after Acceptance of DoDIN Protection / Cybersecurity Assessment | Distribution D | **CUI** | One Time; updated as required |
| Cybersecurity Requirements Definition \* | | Government Determined Format | 30 days after Acceptance of Test Environment Planning and Assessment | Distribution D | **CUI** | One Time; updated as required |
| Incident Response Plan and Procedures \*\* | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Test Environment Planning and Assessment | Distribution D | **CUI** | One Time; updated as required |
| Integration and Acceptance Testing(I/AT) \* | | Government Determined Format | 60 days after Test Environment Planning and Assessment | Distribution D | **CUI** | One Time; updated as required |
| Recommended Production Configuration Changes \*\* | | Contractor Determined Format | 15 days after Integration & Acceptance Testing (I/AT) | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Limited Fielding Implementation Plan \* | | Government Determined Format | 45 days after Acceptance of Authority to Operate | Distribution D | **CUI** | One Time; updated as required |
| System & Configuration Definition (i.e. – “As Built”) \* | | Contractor Determined / Government Approved Format | 45 days after Acceptance of Authority to Operate | Distribution D | **CUI** | Monthly; as required |
| Defect Tracking List \* | | Contractor Determined Format | 45 days after Acceptance of Authority to Operate | Distribution D | **CUI** | Weekly; as required |
| Evergreen Strategy \* | | Government Determined Format | Ongoing after FOC Declaration until the end of the contract | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Usage Reports (by feature capability) \* | | Contractor Determined Format | Ongoing after FOC Declaration until the end of the contract | Distribution D Distribution F | **CUI** | Monthly; as required |
| Incident Reports \* | | Contractor Determined / Government Approved Format | Ongoing after FOC Declaration until the end of the contract | Distribution D | **CUI** | Weekly; as required |
| FISMA Reporting and Updates \*/† | | Government Determined Format | Ongoing after FOC Declaration until the end of the contract | Distribution D | **CUI** | Yearly; as required |
| FEDRAMP Reporting and Updates \*/† | | Government Determined Format | Ongoing after FOC Declaration until the end of the contract | Distribution D | **CUI** | Yearly; as required |
| *Add rows as needed*  *[Insert Deliverable Title & Indicate level of responsibility based on ------]* | | *[Identify Format Type that w* |  | *[Insert distribution in accordance with DoDM 5200.01 Vol 4 and DoDM 5230.24]* | *[Insert classification marking in accordance with DoDM 5200.01 Vol4 DoDM 5230.24]* | [ |
| Symbol: | Definition: | | | | | |
| \* | 50% Government responsibility and 50% contractor responsibility | | | | | |
| \*\* | 100% Contractor responsibility | | | | | |
| † | These artifacts are built upon the packages submitted as part of the vendor's DoD PA | | | | | |

## Task 2 – SIPRNet Environment

The contractor shall deliver a CSO that enables collaboration across the DoD enterprise. The SIPRNet CSO shall include System Wide, Core Services (i.e., email, IM/chat, web conferencing, native audio, native video, content management, and productivity suite), and DoDIN Protection requirements IAW the FRD sections 1, 2, and 3,

having a network category of “Both” or “SIPR”. Furthermore, the contractor shall be required to interface the CSO to the core integration points identified in the FRD section 6. Lastly, the contractor shall adhere to the

performance objectives identified in the FRD section 8, and shall be required to perform testing activities/events (i.e., integration, acceptance, operational) IAW the FRD section 9, to verify the proper interoperability between the CSO and core integration points (FRD section 6).

#### Subtask 1 – United States Territories and Possessions

Provide geographically dispersed off-premises CSO within a DoD private/community cloud that meets Impact Level 6 requirements in accordance with the DoD CC SRG and the FRD.

#### Subtask 2 – Locations outside of the United States Territories and Possessions

Provide a geographically dispersed DoD private/community CSO that is deployed in DoD facilities using an

***on-premises*** deployment model that meets Impact Level 6 in accordance with the DoD CC SRG and FRD.

#### Deliverables

The Government shall require the following documents as key deliverables for this task and sub-tasks. All deliverables listed below correspond with the key program milestones, activates, and deliverables listed in Attachment D. Any additional deliverables (i.e. not indicated below or in attachment D) maybe required by the Government based on the proposed technical/management approach and will be included at task order execution.

*[The contractor shall propose any additional deliverables based upon their technical and management approach that collectively provide sufficient evidence of satisfactory performance of activities required for this task and sub-tasks as applicable. Any additional deliverables included within the table below should also be included in key program milestone, activities, and deliverables list Attachment D]*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Deliverable Name** | | **Format** | **Due Date (Notional)** | **Distribution** | **Classification** | **Frequency** |
| Architecture, DoDAF Artifacts/Diagrams (AV, OV, SV, StdV, CV) \* | | Government Determined Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| System Design Document \*\* | | Government Determined Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Interfaces, Ports & Protocols Baseline \*\* | | Contractor Determined Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Service Support Functions and Integration Plan \* | | Contractor Determined / Government Approved Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Performance Monitoring Strategy \* | | Contractor Determined / Government Approved Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Security Architecture Analysis \* | | Contractor Determined / Government Approved Format | 30 days after Task Order Execution | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Communication Plan \* | | Contractor Determined / Government Approved Format | 30 days after Task Order Execution | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Migration Schedule \* | | Contractor Determined Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Service Management Plan \*\* (To Address: Access Management,  Event Management,  Incident Management,  Request Fulfillment,  Storefront Integration,  Service Desk Support  Network Operations (NetOps)  Service Desk Integration (i.e., GSD and/or Mission Partner) OSS/JMN and Out of Band (OOB) management) | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Preliminary Design Review | Distribution D | **CUI** | One Time; updated as required |
| Change Management Plan \* | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Tenancy Review | Distribution D | **CUI** | One Time; updated as required |
| Incident Response Plan and Procedures \* | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Tenancy Review | Distribution D | **CUI** | One Time; updated as required |
| Service Desk Strategy \* | | Contractor Determined Format | 30 days after Acceptance of Tenancy Review | Distribution D | **CUI** | One Time; updated as required |
| System Administrator Configuration Guides for SIPR \* | | Contractor Determined / Government Approved Format | 15 days after Acceptance of Production Readiness Review | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Impact Assessment Report \* | | Government Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Implementation Status Report \* | | Contractor Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Implemented Cybersecurity Controls Checklist \* | | Contractor Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Cybersecurity Assessment Report \* | | Government Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Selected Security Control Assessment \* | | Government Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Issue Resolution/Remediation Report \* | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Risk Acceptance Recommendation \* | | Contractor Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Continuous monitoring strategy/plan \*\*/† | | Government Determined Format | 30 days after Acceptance of Provisional Authorization | Distribution D | **CUI** | One Time; updated as required |
| System Security Plan (SSP) \*\* | | Government Determined Format | 30 days after Acceptance of Provisional Authorization | Distribution D | **CUI** | One Time; updated as required |
| Directory Replication Plan \*\* | | Contractor Determined Format | 45 days after Acceptance of Provisional Authorization | Distribution D | **CUI** | One Time; updated as required |
| OCSP/CRL Integration Plan \* | | Contractor Determined Format | 45 days after Acceptance of Provisional Authorization | Distribution D | **CUI** | One Time; updated as required |
| Provisioning / Authentication Assessment Documentation \*/† | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Yearly; as required |
| Privacy Impact Assessment \*/† | | Government Determined Format | 15 days after IdAM Integration | Distribution D | **CUI** | Yearly; as required |
| Privacy Threshold Analysis \*/† | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Yearly; as required |
| Residual Risk Statement \*/† | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Yearly; as required |
| Vulnerability Assessment \*/† | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Monthly; as required |
| Business Impact Analysis \* | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Monthly; as required |
| Contingency Plan \* | | Contractor Determined / Government Approved Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Monthly; as required |
| Continuous Monitoring Test Plan \*/† | | Contractor Determined / Government Approved Format | 30 days after Acceptance of DoDIN Protection / Cybersecurity Assessment | Distribution D | **CUI** | One Time; updated as required |
| Cybersecurity Requirements Definition \* | | Government Determined Format | 30 days after Acceptance of Test Environment Planning and Assessment | Distribution D | **CUI** | One Time; updated as required |
| Incident Response Plan and Procedures \*\* | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Test Environment Planning and Assessment | Distribution D | **CUI** | One Time; updated as required |
| Integration and Acceptance Testing(I/AT) \* | | Government Determined Format | 60 days after Acceptance of Test Environment Planning and Assessment | Distribution D | **CUI** | One Time; updated as required |
| Recommended Production Configuration Changes \*\* | | Contractor Determined Format | 15 days after Acceptance of Integration & Acceptance Testing (I/AT) | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Limited Fielding Implementation Plan \* | | Government Determined Format | 45 days after Acceptance of Authority to Operate | Distribution D | **CUI** | One Time; updated as required |
| System & Configuration Definition (i.e. – “As Built”) \* | | Contractor Determined / Government Approved Format | 45 days after Acceptance of Authority to Operate | Distribution D | **CUI** | Monthly; as required |
| Defect Tracking List \* | | Contractor Determined Format | 45 days after Acceptance of Authority to Operate | Distribution D | **CUI** | Weekly; as required |
| Evergreen Strategy \* | | Government Determined Format | Ongoing after FOC Declaration until the end of the contract | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Usage Reports (by feature capability) \* | | Contractor Determined Format | Ongoing after FOC Declaration until the end of the contract | Distribution D Distribution F | **CUI** | Monthly; as required |
| Incident Reports \* | | Contractor Determined / Government Approved Format | Ongoing after FOC Declaration until the end of the contract | Distribution D | **CUI** | Weekly; as required |
| FISMA Reporting and Updates \*/† | | Government Determined Format | Ongoing after FOC Declaration until the end of the contract | Distribution D | **CUI** | Yearly; as required |
| FEDRAMP Reporting and Updates \*/† | | Government Determined Format | Ongoing after FOC Declaration until the end of the contract | Distribution D | **CUI** | Yearly; as required |
| *[Insert Deliverable Title & Indicate level of responsibility based on ------]* | | *[Identify Format Type that* |  |  |  |  |
| *Add rows as needed* | |  |  |  |  |  |
| Symbol: | Definition: | | | | | |
| \* | 50% Government responsibility and 50% contractor responsibility | | | | | |
| \*\* | 100% Contractor responsibility | | | | | |
| † | These artifacts are built upon the packages submitted as part of the vendor's DoD PA | | | | | |

## Task 3 – Denied, Disconnected, Intermittent, Limited Bandwidth (D-DIL) Environment

The contractor shall provide a solution able to operate when disconnected from the main CSO that allows for

continuity of operations while experiencing a Denied, Disconnected, Intermittent or Limited Bandwidth condition IAW section 5 and appendix A of the FRD.

In many cases, the full suite of DEOS services may not be required and in some cases the requirements may

consist of a single function deployed as a standalone service (i.e., black-box, hardware, software, etc.) that may be the primary provider of the service for an extended period of time. The contractor shall plan for these variations in D-DIL service based on a per tenancy or standalone environments that are implemented.

#### Subtask 1 – D-DIL Prototype

Engineer, configure, and deploy a prototype for the D-DIL use cases in appendix A of the FRD for NIPRNet and SIPRNet environments. The prototype shall demonstrate the functionality and provide the ability to validate the technical feasibility for the D-DIL use cases. The prototype shall have all the functionality of the D-DIL

product/solution and capable of supporting real-world scenarios.

#### Subtask 2 – NIPRNet D-DIL Environment

Engineer, configure and deploy a standalone, independently operable D-DIL solution that communicates with the NIPRNet CSO when connectivity is regained to synchronize data. D-DIL deployments may experience lower cloud service availability.

#### Subtask 3 – SIPRNet D-DIL Environment

Engineer, configure and deploy a standalone, independently operable D-DIL solution that communicates with the SIPRNet CSO when connectivity is regained to synchronize data. D-DIL deployments may experience lower cloud service availability.

#### Subtask 4 – D-DIL Software/Subscription Licenses

The contractor shall offer annual subscription licenses using a fixed fee for small, medium, and large user

populations.

#### Subtask 5 – Infrastructure

The contractor shall offer a pricing model for the software, hardware and virtual infrastructure required to enable D-DIL instances for the following three scalability models: small D-DIL deployments consisting of less than 300 personnel; medium D-DIL deployments consisting of 300 -1,500 personnel; and large D-DIL deployments

consisting of 1,500 - 6,000 personnel.

#### Deliverables

The Government shall require the following documents as key deliverables for this task and sub-tasks. All deliverables listed below correspond with the key program milestones, activates, and deliverables listed in Attachment D. Any additional deliverables (i.e. not indicated below or in attachment D) maybe required by the Government based on the proposed technical/management approach and will be included at task order execution.

*[The contractor shall propose any additional deliverables based upon their technical and management approach that collectively provide sufficient evidence of satisfactory performance of activities required for this task and sub-tasks as applicable. Any additional deliverables included within the table below should also be included in key program milestone, activities, and deliverables list Attachment D]*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Deliverable Name** | | **Format** | **Due Date (Notional)** | **Distribution** | **Classification** | **Frequency** |
| Architecture, DoDAF Artifacts/Diagrams (AV, OV, SV, StdV, CV) \* | | Government Determined Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| System Design Document \*\* | | Government Determined Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Interfaces, Ports & Protocols Baseline \*\* | | Contractor Determined Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Service Support Functions and Integration Plan \* | | Contractor Determined / Government Approved Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| D-DIL Architecture/ Integration Plan \* | | Government Determined Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Performance Monitoring Strategy \* | | Contractor Determined / Government Approved Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Security Architecture Analysis \* | | Contractor Determined / Government Approved Format | 30 days after Task Order Execution | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Communication Plan \* | | Contractor Determined / Government Approved Format | 30 days after Task Order Execution | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Migration Schedule \* | | Contractor Determined Format | 30 days after Task Order Execution | Distribution D | **CUI** | One Time; updated as required |
| Service Management Plan \*\* (To Address: Access Management,  Event Management,  Incident Management,  Request Fulfillment,  Storefront Integration,  Service Desk Support  Network Operations (NetOps)  Service Desk Integration (i.e., GSD and/or Mission Partner) OSS/JMN and Out of Band (OOB) management) | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Preliminary Design Review | Distribution D | **CUI** | One Time; updated as required |
| Change Management Plan \* | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Tenancy Review | Distribution D | **CUI** | One Time; updated as required |
| Incident Response Plan and Procedures \* | | Contractor Determined / Government Approved Format | 30 days after Tenancy Review | Distribution D | **CUI** | One Time; updated as required |
| Service Desk Strategy \* | | Contractor Determined Format | 30 days after Acceptance of Tenancy Review | Distribution D | **CUI** | One Time; updated as required |
| System Administrator Configuration Guides for NIPR/SIPR D-DIL Environments\* | | Contractor Determined / Government Approved Format | 15 days after Acceptance of Production Readiness Review | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Impact Assessment Report \* | | Government Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Implementation Status Report \* | | Contractor Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Implemented Cybersecurity Controls Checklist \* | | Contractor Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Cybersecurity Assessment Report \* | | Government Determined Format | 30 days after Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Selected Security Control Assessment \* | | Government Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Issue Resolution/Remediation Report \* | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Risk Acceptance Recommendation \* | | Contractor Determined Format | 30 days after Acceptance of Production Readiness Review | Distribution D | **CUI** | One Time; updated as required |
| Continuous monitoring strategy/plan \*\*/† | | Government Determined Format | 30 days after Acceptance of Provisional Authorization | Distribution D | **CUI** | One Time; updated as required |
| System Security Plan (SSP) \*\* | | Government Determined Format | 30 days after Acceptance of Provisional Authorization | Distribution D | **CUI** | One Time; updated as required |
| Directory Replication Plan \*\* | | Contractor Determined Format | 45 days after Provisional Authorization | Distribution D | **CUI** | One Time; updated as required |
| OCSP/CRL Integration Plan \* | | Contractor Determined Format | 45 days after Acceptance of Provisional Authorization | Distribution D | **CUI** | One Time; updated as required |
| Provisioning / Authentication Assessment Documentation \*/† | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Yearly; as required |
| Privacy Impact Assessment \*/† | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Yearly; as required |
| Privacy Threshold Analysis \*/† | | Government Determined Format | 15 days afte IdAM Integration | Distribution D | **CUI** | Yearly; as required |
| Residual Risk Statement \*/† | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Yearly; as required |
| Vulnerability Assessment \*/† | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Monthly; as required |
| Business Impact Analysis \* | | Government Determined Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Monthly; as required |
| Contingency Plan \* | | Contractor Determined / Government Approved Format | 15 days after Acceptance of IdAM Integration | Distribution D | **CUI** | Monthly; as required |
| Continuous Monitoring Test Plan \*/† | | Contractor Determined / Government Approved Format | 30 days after Acceptance of DoDIN Protection / Cybersecurity Assessment | Distribution D | **CUI** | One Time; updated as required |
| Cybersecurity Requirements Definition \* | | Government Determined Format | 30 days after Test Environment Planning and Assessment | Distribution D | **CUI** | One Time; updated as required |
| Incident Response Plan and Procedures \*\* | | Contractor Determined / Government Approved Format | 30 days after Acceptance of Test Environment Planning and Assessment | Distribution D | **CUI** | One Time; updated as required |
| Integration and Acceptance Testing (I/AT) \* | | Government Determined Format | 60 days after Acceptance of Test Environment Planning and Assessment | Distribution D | **CUI** | One Time; updated as required |
| Recommended Production Configuration Changes \*\* | | Contractor Determined Format | 15 days after Acceptance of Integration & Acceptance Testing (I/AT) | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Limited Fielding Implementation Plan \* | | Government Determined Format | 45 days after Acceptance of Authority to Operate | Distribution D | **CUI** | One Time; updated as required |
| System & Configuration Definition (i.e. – “As Built”) \* | | Contractor Determined / Government Approved Format | 45 days after Acceptance of Authority to Operate | Distribution D | **CUI** | Monthly; as required |
| Defect Tracking List \* | | Contractor Determined Format | 45 days after Acceptance of Authority to Operate | Distribution D | **CUI** | Weekly; as required |
| Evergreen Strategy \* | | Government Determined Format | Ongoing after FOC Declaration until the end of the contract | Distribution D Distribution F | **CUI** | One Time; updated as required |
| Usage Reports (by feature capability) \* | | Contractor Determined Format | Ongoing after FOC Declaration until the end of the contract | Distribution D Distribution F | **CUI** | Monthly; as required |
| Incident Reports \* | | Contractor Determined / Government Approved Format | Ongoing after FOC Declaration until the end of the contract | Distribution D | **CUI** | Weekly; as required |
| *[Insert Deliverable Title & Indicate level of responsibility based on ------]* | | *[Identify Format Type that* |  |  |  |  |
| *Add rows as needed* | |  |  |  |  |  |
| Symbol: | Definition: | | | | | |
| \* | 50% Government responsibility and 50% contractor responsibility | | | | | |
| \*\* | 100% Contractor responsibility | | | | | |
| † | These artifacts are built upon the packages submitted as part of the vendor's DoD PA | | | | | |

## Task 4 – User Tenancy Structure

The Government will allow flexibility and expects the contractor to propose a tenancy[[1]](#footnote-1) structure. As a result, the contractor shall propose an architecture, which meets the requirements of the FRD, and allows each Combatant Commands, Services and Agencies (CC/S/As) the ability to apply controls and restrictions for their users and data, site configuration, as well as user, feature, and functionality management to meet their mission needs. This includes the ability to grant/remove administrative privileges, user roles, and the ability to control license

assignment within the solution. The Government requires a tenancy structure to support approximately 3.15

million subscriber’s part of the DoD enterprise.

#### Deliverables

The Government shall require the following documents as key deliverables for this task and sub-tasks. All deliverables listed below correspond with the key program milestones, activates, and deliverables listed in Attachment D. Any additional deliverables (i.e. not indicated below or in attachment D) maybe required by the Government based on the proposed technical/management approach and will be included at task order execution.

*[The contractor shall propose any additional deliverables based upon their technical and management approach that collectively provide sufficient evidence of satisfactory performance of activities required for this task and sub-tasks as applicable. Any additional deliverables included within the table below should also be included in key program milestone, activities, and deliverables list Attachment D]*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Deliverable Title | | Format | **Due Date** | **Distribution** | **Classification Marking** | **Frequency** |
| Tenancy Execution Plan \*\* | | Contractor Determined Format | 30 days after Acceptance of Preliminary Design Review | Distribution D | CUI | One Time, updated as needed |
| Service Management Plan \* | | Contractor Determined Format | 30 Calendar Days after Preliminary Design Review | Distribution D | CUI | One Time; Updated  annually as required |
| Multiple/Split Domain Management  Approach \* | | Contractor Determined Format | 30 Calendar Days after Preliminary Design Review | Distribution D | CUI | One Time; updated as required |
| Briefing Slides \*\* | | Government Determined Format | 30 Calendar Days after TO Execution | Distribution D | CUI | Weekly, as required |
| *[Insert Deliverable Title & Indicate level of responsibility based on ------]* | | *[Identify Format Type that* |  |  |  |  |
| *Add rows as needed* | |  |  |  |  |  |
| Symbol: | Definition: | | | | | | |
| \* | 50% Government responsibility and 50% contractor responsibility | | | | | | |
| \*\* | 100% Contractor responsibility | | | | | | |
| † | These artifacts are built upon the packages submitted as part of the vendor's DoD PA | | | | | | |

## Task 5 – Subscription Licenses

The contractor shall propose a per-seat subscription-based pricing, and a corresponding licensing model in

accordance with Table 9 – Notional Core Service User Tiers, which allows the Government to purchase or subscribe to the contractor CSO for a specific period and for a set price.

#### Subtask 1 – Core Services

The contractor shall provide a per subscription based licensing structure for the functionality outlined in Figure 1. The exact number of users within each licensing tier will be specified at the task order-level upon task order execution. In addition to Figure 1, the contractor shall reference the information presented in Table 9 – Notional Core Service User Tiers, to propose a licensing structure that maps to the CSO’s commercial licensing structure. Table 9 should be used as a ***reference only*** for the licensing structure the Government is requesting.

**Table 9 – Notional Core Service User Tiers**

|  |  |  |
| --- | --- | --- |
| Type of User | Features Breakdown | **Types of Clients** |
| **Economy User** | Messaging capabilities (i.e., email, calendar, contacts) to include required legal administrative functions associated with e-discovery and records retentions. | * Web Browser only |
| **Basic User** | All Economy User capabilities plus content management (i.e., web portal; file sharing storage and archive; index, search and filter; and workflows and orchestration) and productivity suite (i.e., word processor, spreadsheet, and presentation). | * Web Browser only |
| **Business User** | All Basic User capabilities plus collaboration (i.e., one-to-one instant message, presence, persistent group chat, web conferencing, white boarding, and desktop sharing) and native audio and video. | * Standalone/Thick * Mobile App(s) * Virtual Desktop * Web Browser |
| **Enterprise User** | All Business User capabilities plus voice (i.e., business voice, business voice conferencing, voicemail, and unified messaging) and video (i.e., business video and business video conferencing). | * Standalone/Thick * Mobile App (s) * Virtual Desktop * Web Browser |

#### Subtask 2 – Drafting and Diagramming

The contractor shall provide a per user license for Drafting and Diagramming services that assist with the creation of diagrams, flow and organizational charts.

#### Subtask 3 – Project Management

The contractor shall provide a per user license for Project Management services that assist with assigning

resources to tasks and tracking project progress.

#### Subtask 4 – Other Services/Add-Ons/Plug-Ins

In addition to the tiered user licensing structure identified for sub-task(s) 5.6.1, 5.6.2, and 5.6.3 the contractor shall independently indicate in Attachment 6 any additional service add-ons, plugins, licenses (e.g., Geographic information system) that can be purchased with the proposed CSO.

#### Deliverables

The Government shall require the following documents as key deliverables for this task and sub-tasks. All deliverables listed below correspond with the key program milestones, activates, and deliverables listed in Attachment D. Any additional deliverables (i.e. not indicated below or in attachment D) maybe required by the Government based on the proposed technical/management approach and will be included at task order execution.

*[The contractor shall propose any additional deliverables based upon their technical and management approach that collectively provide sufficient evidence of satisfactory performance of activities required for this task and sub-tasks as applicable. Any additional deliverables included within the table below should also be included in key program milestone, activities, and deliverables list Attachment D]*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Deliverable Title | | Format | **Due Date** | **Distribution** | **Classification Marking** | **Frequency** |
|  | Software License Management Plan \*\* | | Contractor Determined Format | 30 Calendar Days after TO Execution | Distribution D | CUI | One Time; Updated annually as required |
|  | Software License  Reports \*\* | | Contractor Determined / Government Approved Format | Monthly, on 5th workday after TO  Execution | Distribution D | CUI | Monthly, or as required |
|  | Licensing &  Subscription  Structure \*\* | | Contractor Determined Format | 30 Calendar Days after TO Execution | Distribution D | CUI | One Time; Updated annually as  Required |
|  | Briefing Slides \*\* | | Contractor Determined Format | 30 Calendar Days after TO Execution | Distribution D | CUI | Weekly, as required |
|  | *[Insert Deliverable Title & Indicate level of responsibility based on ------]* | | *[Identify Format Type that* |  |  |  |  |
|  | *Add rows as needed* | |  |  |  |  |  |
| Symbol: | | Definition: | | | | | |
| \* | | 50% Government responsibility and 50% contractor responsibility | | | | | |
| \*\* | | 100% Contractor responsibility | | | | | |
| † | | These artifacts are built upon the packages submitted as part of the vendor's DoD PA | | | | | |

## Task 6 – Additional Supporting Infrastructure, Integration Points, and Services

The contractor shall be required to interoperate the proposed CSO with the following supporting infrastructure, integration points, and services based on user demand at the task order-level upon task order execution:

#### Subtask 1 – Enterprise Voice Over Internet Protocol (EVoIP)

The contractor shall leverage the SS backbone to interface the NIPRNet CSO to the DISA Enterprise Voice over IP (EVoIP) infrastructure, IAW the FRD section 7.1.3 and SOO section 5.6.7, Subtask 7 – Softswitch (SS) Backbone.

#### Subtask 2 – Enterprise Classified Voice over IP (ECVoIP)

The contractor shall interoperate the SIPRNet CSO to ECVoIP Session Managers by establishing SIP trunks IAW the FRD section 7.1.4.

#### Subtask 3 – Mass Warning Notification

The contractor shall provide integration or interoperability with Service or Component mass warning notification systems IAW the FRD section 7.6.

#### Subtask 4 – Local Voice Survivability

The contractor shall provide continuity of voice services and local voice survivability when the B/P/C/S is

severed from the DISN, IAW the FRD section 7.1.6

#### Subtask 5 – E-911

The contractor shall ensure E-911 calls originated from soft clients, can be routed to the Public Safety Answering Point (PSAP), or local B/P/C/S Emergency Response Centers (ERCs) IAW the FRD section 7.1.5.

**Note:** Specific E-911 services, such as national Private Switch-Automatic Location Information (PS ALI), local PS ALI (when offered), and location discovery capabilities, are expected to be provided through already

established contract vehicles (e.g., Networx contract) outside of the DEOS contract.

#### Subtask 6 – Voice Over Secure IP (VoSIP)

The contractor shall interoperate the SIPRNet CSO to VoSIP Session Managers by establishing SIP trunks IAW the FRD section 7.1.7.

#### Subtask 7 – Softswitch (SS) Backbone

The contractor shall interoperate the NIPRNet CSO to the SS backbone by using one of the following methods:

Configure a SIP Trunk to the Government provided SBCs, if the Government provided APL certified SBCs could translate DEOS CSO signaling traffic to AS-SIP.

Provide an AS-SIP Gateway, to translate DEOS CSO proprietary based signaling traffic to AS-SIP.

In addition, the contractor shall support E.164 number routing, the DoD’s World-Wide Numbering & Dial Plan, and shall assign Defense Switched Network (DSN) and commercial phone numbers to subscribers/end

instruments in accordance with the FRD section 7.1 and SOO section 5.6.7 Subtask 7 – Softswitch (SS) Backbone.

#### Subtask 8 – Voice Internet Service Provider (VISP) / Commercial Voice Networks (PSTN)

The contractor shall leverage the SS backbone to interface the NIPRNet CSO to the DISA Voice Internet Service Provider (VISP), which provides Public Switched Telephone Network (PSTN) access to DoD IAW the FRD

section 7.1.2 and SOO section 5.6.7 Subtask 7 – Softswitch (SS) Backbone.

#### Subtask 9 – Local Base/Post/Camp/Station Session Controllers

The contractor shall interoperate the NIPRNet CSO to individual Local Session Controllers (LSCs) on an as needed basis per CC/S/A by establishing SIP trunks IAW the DEOS FRD section 7.1.8.

#### Subtask 10 – Unclassified Video Interoperability

The contractor shall interoperate the NIPRNet CSO to the SS backbone to enable video communications IAW the FRD section 7.2.1.

#### Subtask 11 – Classified Video Interoperability

The contractor shall interoperate the SIPRNet CSO to DISA ECVoIP Session Managers to enable video

communications IAW the FRD section 7.2.2.

#### Subtask 12 – NIPR Local B/P/C/S Provided VTC Systems

The contractor shall interoperate the NIPRNet CSO to local base/post/camp/station provided VTC systems IAW the FRD section 7.2.3.

#### Subtask 13 – SIPR Local B/P/C/S Provided VTC Systems

The contractor shall interoperate the SIPRNet CSO to local base/post/camp/station provided VTC systems IAW the FRD section 7.2.3.

#### Subtask 14 – NIPR Global Content Directory Services (GCDS)

The contractor shall leverage the GCDS to accelerate the delivery of NIPRNet CSO content and applications across the DoDIN IAW the FRD section 7.4.

#### Subtask 15 – SIPR Global Content Directory Services (GCDS)

The contractor shall leverage the GCDS to accelerate the delivery of SIPRNet CSO content and applications across the DoDIN IAW the FRD section 7.4.

#### Subtask 16 – NIPR IM, Chat & Presence Federation

The contractor shall facilitate IM, Chat & Presence Federation of the NIPRNet CSO with external NIPR chat

systems IAW the FRD section 7.5.

#### Subtask 17 – SIPR IM, Chat & Presence Federation

The contractor shall facilitate IM, Chat & Presence Federation of the SIPRNet CSO with external SIPRNet chat systems IAW the FRD section 7.5.

#### Subtask 18 – Records Management

Configure the CSO to support NARA requirements IAW [DoDI 5015.02](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/501502p.pdf), and the FRD section 4.

#### Subtask 19 – Workflow

Configure the CSO to support declassification review, legal-related reviews, and approval processes IAW the FRD section 4.1.

#### Subtask 20 – Redaction

Configure the CSO to support Document Redaction IAW the FRD section 4.2.

#### Subtask 21 – Freedom of Information Act (FOIA)

Provide enhanced FOIA functionality as part of the enhanced Records Management capability provided by the CSO IAW the FRD section 4.3.

#### Subtask 22 – eDiscovery

Configure the CSO to support documentation-marking, redactions, and deduplication of files IAW the FRD section 4.4.

#### Subtask 23 – Voicemail

Provide industry standard voicemail for DEOS subscribers IAW the FRD section 7.1.10.

#### Subtask 24 – Unified Messaging

Integrate the DEOS provided voicemail with the DEOS provided email to provide unified messaging. Both voicemail and email services must be provided by the same CSO. Otherwise, at the customer request, integrate the DEOS provided email with non-DEOS provided voicemail systems to provide unified messaging IAW the FRD section 7.1.11.

#### Deliverables

The Government shall require the following documents as key deliverables for this task and sub-tasks. All deliverables listed below correspond with the key program milestones, activates, and deliverables listed in Attachment D. Any additional deliverables (i.e. not indicated below or in attachment D) maybe required by the Government based on the proposed technical/management approach and will be included at task order execution.

*[The contractor shall propose any additional deliverables based upon their technical and management approach that collectively provide sufficient evidence of satisfactory performance of activities required for this task and sub-tasks as applicable. Any additional deliverables included within the table below should also be included in key program milestone, activities, and deliverables list Attachment D]*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Deliverable Title | | Format | **Due Date** | **Distribution** | **Classification Marking** | **Frequency** |
| Integration Plan \*\* | | Contractor Determined  Format | 30 Calendar Days after Critical Design Review | Distribution D | CUI | One Time; Updated annually as  required |
| Infrastructure  Review Checklist \*\* | | Contractor Determined  Format | 30 Calendar Days after Critical Design Review | Distribution D | CUI | One Time; Updated annually as  required |
| Infrastructure  Analysis/Evaluation Report \*\* | | Contractor Determined  Format | 30 Calendar Days after Critical Design Review | Distribution D | CUI | One Time; Updated annually as  required |
| Engineering Artifacts \*\* | | Contractor Determined  Format | 30 Calendar Days after Critical Design Review | Distribution D | CUI | One Time; Updated annually as  required |
| White Papers \*\* | | Contractor Determined  Format | 30 Calendar Days after Critical Design Review | Distribution D | CUI | One Time; Updated annually as  required |
| Architecture, DoDAF  Artifacts/Diagrams (AV, OV, SV, StdV, CV) \*\* | | Contractor Determined Format | 90 Calendar Days after TO Execution | Distribution D | CUI | One Time; Updated annually as  required |
| Interfaces, Ports & Protocols Baseline \*\* | | Contractor Determined Format | 90 Calendar Days after TO Execution | Distribution D | CUI | One Time; Updated annually as  required |
| Cybersecurity  Monitoring  Strategy \*\* | | Contractor Determined Format | 30 Calendar Days after TO Execution | Distribution D | CUI | One Time; Updated annually as  required |
| Transition/  Decommission Plan \*\* | | Contractor Determined Format | 30 Calendar Days after TO Execution | Distribution D | CUI | One Time; Updated annually as  required |
| *[Insert Deliverable Title & Indicate level of responsibility based on ------]* | | *[Identify Format Type that* |  |  |  |  |
| *Add rows as needed* | |  |  |  |  |  |
| Symbol: | Definition: | | | | | |
| \* | 50% Government responsibility and 50% contractor responsibility | | | | | |
| \*\* | 100% Contractor responsibility | | | | | |
| † | These artifacts are built upon the packages submitted as part of the vendor's DoD PA | | | | | |

## Task 7 – Data Migration & Readiness Assessments

The contractor shall perform a comprehensive evaluation of CC/S/A data, to prepare the environment for

migration to DEOS. Evaluations shall clearly outline migration traffic flows, involved system components,

applications, and integration dependencies.

#### Subtask 1 – Directory Service

The contractor shall analyze the existing enterprise directory, and as needed, customer specific directories, to outline the necessary execution activities, migration strategy, implementation plan, and configuration changes required to optimize the existing directory environment and support the successful migration of directory data into the new DEOS service. Examples include directory object normalization, non-person entity (NPE) standardization, and attributes cleanup/mapping to allow synchronization with the new DEOS service.

The contractor shall configure the DEOS service to authenticate users IAW the FRD requirements (e.g., PIV

certificate, alternate DoD approved persona-specific authenticator or persona-specific assertion, DoD approved multifactor authentication, or username/password) as directed by the Government IAW DoDI 8500.1 and DoDI 8520.03.

DEOS directories and authentication methods shall support the use of current DoD approved Public Key

Infrastructure (PKI) mechanisms (e.g., PKI, Common Access Cards (CACs), SIPR Tokens and derived

credentials) for authentication on virtual desktops, web browsers, thick clients, and DoD approved mobile

platforms, and shall check for certificate expiration, against a DoD Certificate Authority (CA) that issued the

certificate, confirming the certificate has not been revoked.

#### Subtask 2 – Email

The contractor shall assess existing email environments and data to ensure an optimal migration. Examples of

activities include, but are not limited to, evaluating email profiles, email data volume, PST data volume, and cleanup of mailboxes, distribution lists and delegations clearly identified by the Government.

#### Subtask 3 – Content Management

The contractor shall analyze existing content management environments and data to ensure an optimal migration. Examples of activities include, but are not limited to, site structure/content analysis, site content volume,

identification and cleanup of folder hierarchies, determining user permissions, and evaluate existing workflows.

#### Deliverables

The Government shall require the following documents as key deliverables for this task and sub-tasks. All deliverables listed below correspond with the key program milestones, activates, and deliverables listed in Attachment D. Any additional deliverables (i.e. not indicated below or in attachment D) maybe required by the Government based on the proposed technical/management approach and will be included at task order execution.

*[The contractor shall propose any additional deliverables based upon their technical and management approach that collectively provide sufficient evidence of satisfactory performance of activities required for this task and sub-tasks as applicable. Any additional deliverables included within the table below should also be included in key program milestone, activities, and deliverables list Attachment D]*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Deliverable Title | | Format | **Due Date** | **Distribution** | **Classification Marking** | **Frequency** |
|  | Core Capability Data Readiness Plan \*\* | | Contractor Determined Format | Draft 45 Calendar Days after TO Execution | Distribution D | CUI | One Time; Updated annually as required |
|  | Core Capability Data Readiness  Review Checklist \*\* | | Contractor Determined Format | Draft 45 Calendar Days after TO Execution | Distribution D | CUI | One Time; Updated monthly as Required |
|  | Core Capability Analysis/Evaluation Report \*\* | | Contractor Determined Format | Draft 45 Calendar Days after TO Execution | Distribution D | CUI | One Time; Updated monthly as required |
|  | *[Insert Deliverable Title & Indicate level of responsibility based on ------]* | | *[Identify Format Type that* |  |  |  |  |
|  | *Add rows as needed* | |  |  |  |  |  |
| Symbol: | | Definition: | | | | | |
| \* | | 50% Government responsibility and 50% contractor responsibility | | | | | |
| \*\* | | 100% Contractor responsibility | | | | | |
| † | | These artifacts are built upon the packages submitted as part of the vendor's DoD PA | | | | | |

## Task 8 – User & Data Migration

The contractor shall develop a data migration plan that minimizes the business impact to day-to-day operations such as downtime, data integrity issues, and costs. The contractor shall provide the manpower, tools, and

hardware needed to migrate existing services, operations, and customer data necessary to deliver the CSO to

approximately 3.15 million DoD subscribers. During migration, the contractor shall support dual operations,

ensuring that users migrated to the CSO are able to collaborate with those that have not been migrated. In

addition, the contractor shall ensure that customer profiles and data stored on the legacy systems are migrated to the CSO as agreed upon with the Government and to the customer’s satisfaction. The CSO must support the

collection, management, and publishing of information in digital format using a web interface. User/

organizational content may take the form of text (such as electronic documents), multimedia files (such as audio or video files), or any other file type that requires content lifecycle management.

#### Subtask 1 – Directory Service

The contractor shall synchronize user directory data, attributes, certificates, and database objects that support the authentication and authorization required by the CSO. Once synchronization is established, the contractor shall leverage the Enterprise Directory Service (EDS) for provision/de-provisioning of user accounts. The contractor shall provide Government authentication using a Government specified identity provider (IdP). The contractor shall ensure that FRD requirements are being met during migration.

#### Subtask 2 – Email

The contractor shallmigrate user email data, mailboxes, non-person entity (NPE) mailboxes (e.g., conference rooms), group mailboxes, calendars, contact lists and distribution lists from legacy systems. The contractor shall also migrate journaled messages as well as files needed for legal or regulatory compliance. During migration, the contractor shall ensure coexistence of the legacy email systems with the proposed CSO, and shall establish dual delivery of messages during the transition period.

#### Subtask 3 – Content Management

The contractor shallmigrate content management sites, to include structure, content, workflows, and permissions from legacy systems. The contractor shall also migrate files needed for legal or regulatory compliance. The contractor shall ensure coexistence of the legacy content management system with the proposed CSO during

migration.

#### Subtask 4 – Business Voice

The contractor shall migrate legacy DSN and PSTN telephone numbers in E.164 format to subscriber profiles.

#### Subtask 5 – Business Video

The contractor shall migrate legacy DSN and PSTN telephone numbers in E.164 format to DEOS subscriber

profiles.

#### Deliverables

The Government shall require the following documents as key deliverables for this task and sub-tasks. All deliverables listed below correspond with the key program milestones, activates, and deliverables listed in Attachment D. Any additional deliverables (i.e. not indicated below or in attachment D) maybe required by the Government based on the proposed technical/management approach and will be included at task order execution.

*[The contractor shall propose any additional deliverables based upon their technical and management approach that collectively provide sufficient evidence of satisfactory performance of activities required for this task and sub-tasks as applicable. Any additional deliverables included within the table below should also be included in key program milestone, activities, and deliverables list Attachment D]*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Deliverable Title | | Format | **Due Date** | **Distribution** | **Classification Marking** | **Frequency** |
|  | Data Migration & Management Plan/Strategy \* | | Contractor Determined Format | 45 Calendar Days after TO Execution | Distribution D | CUI | One Time;  Updated annually as required |
|  | Monthly User  Migration Reports \*\* | | Contractor Determined Format | Monthly, on 5th workday  after TO  Execution | Distribution D | CUI | Monthly, as  required |
|  | Migration Schedule \*\* | | Contractor Determined Format | Monthly, on 5th workday  after TO  Execution | Distribution D | CUI | Monthly, as  required |
|  | *[Insert Deliverable Title & Indicate level of responsibility based on ------]* | | *[Identify Format Type that* |  |  |  |  |
|  | *Add rows as needed* | |  |  |  |  |  |
| Symbol: | | Definition: | | | | | |
| \* | | 50% Government responsibility and 50% contractor responsibility | | | | | |
| \*\* | | 100% Contractor responsibility | | | | | |
| † | | These artifacts are built upon the packages submitted as part of the vendor's DoD PA | | | | | |

## Task 9 – Training

The contractor shall develop training materials to prepare DEOS subscribers, administrators, and instructors on the CSO features and functions in preparation for migration, deployments and day-to-day operations. The contractor shall develop training artifacts to include Standard Operating Procedures (SOPs), Tactics, Techniques and Procedures (TTPs), and online documentation to train users and administrators on the service.

#### Subtask 1 – Subscriber - Classroom/Instructor Led

Provide in-person, classroom/instructor led training to subscribers. Training content shall include explaining

software features, functions, and common tasks associated with DEOS services and capabilities.

#### Subtask 2 – Subscriber - Individual Hands-On

Provide individual hands-on training to subscribers. Training content shall include explaining software features, functions, and common tasks associated with DEOS services and capabilities.

#### Subtask 3 – Subscriber - Online Instructor Led Training

Provide live online instructor led training to subscribers. Training content shall include explaining software features, functions, and common tasks associated with DEOS services and capabilities.

#### Subtask 4 – Subscriber - Computer Based Training (CBT)

Provide the Government with training materials in digital format (e.g., recorded webinars, factsheets) that can be distributed and published to a web portal, established and maintained by the Government. Provided CBT material shall allow users to troubleshoot and perform common tasks on the service without the need for direct instructor interaction.

#### Subtask 5 – Privileged User- Classroom/Instructor Led

Provide in-person, classroom/instructor led training to Government designated privileged users to explain advanced concepts, software features, and common administrative functions associated with the configuration and management of DEOS services and capabilities.

#### Subtask 6 –Privileged User- Individual Hands-On

Provide individual hands-on training to Government designated privileged users to explain advanced concepts, software features, and common administrative functions associated with the configuration and management of DEOS services and capabilities.

#### Subtask 7 – Privileged User- Online Instructor Led Training

Provide live online instructor led training to Government designated privileged users to explain advanced concepts, software features, and common administrative functions associated with the configuration and management of DEOS services and capabilities.

#### Subtask 8 – Privileged User- Computer Based Training (CBT)

Provide the Government with training materials in digital format (e.g., recorded webinars, factsheets) that can be distributed and published to a web portal, established and maintained by the Government. Provided CBT material shall allow Government designated privileged users to troubleshoot and perform common tasks on the service without the need for direct instructor interaction.

#### Subtask 9 – Trainer - Classroom/Instructor Led

Provide in-person, classroom/instructor led training to Government designated trainers to enable them to explain and train other DEOS subscribers and privileged users on software features, and common functions associated with DEOS services and capabilities.

#### Subtask 10 – Trainer - Individual Hands-On

Provide individual hands-on training to Government designated trainers to enable them to explain and train other DEOS subscribers and privileged users on software features, and common functions associated with DEOS services and capabilities.

#### Subtask 11 – Trainer - Online Instructor Led Training

Provide live online instructor led training to Government designated trainers to enable them to explain and train other DEOS subscribers and privileged users on software features, and common functions associated with DEOS services and capabilities.

#### Subtask 12 – Subscriber - Computer Based Training (CBT)

Provide the Government with training materials in digital format (e.g., recorded webinars, factsheets) that can be distributed and published to a web portal, established and maintained by the Government. Provided CBT material shall allow Government designated trainers to learn software features, and common functions associated with DEOS service, without the need for direct instructor interaction.

#### Deliverables

The Government shall require the following documents as key deliverables for this task and sub-tasks. All deliverables listed below correspond with the key program milestones, activates, and deliverables listed in Attachment D. Any additional deliverables (i.e. not indicated below or in attachment D) maybe required by the Government based on the proposed technical/management approach and will be included at task order execution.

*[The contractor shall propose any additional deliverables based upon their technical and management approach that collectively provide sufficient evidence of satisfactory performance of activities required for this task and sub-tasks as applicable. Any additional deliverables included within the table below should also be included in key program milestone, activities, and deliverables list Attachment D]*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | DeliverableTitle | | Format | **Due Date** | **Distribution** | **Classification Marking** | **Frequency** |
|  | Training  Strategy/Plan \* | | Contractor Determined Format | Draft 45 Calendar Days after TO Execution | Distribution D | CUI | One Time;  Updated  annually as  required |
|  | End User Fact Sheets/Manuals \*\* | | Contractor Determined Format | Monthly, on 5th workday after TO Execution | Distribution D | CUI | Monthly, as  requested |
|  | System  Administrator Configuration Guides for NIPR, SIPR, and D-DIL  Environments \*\* | | Contractor Determined Format | Monthly, on 5th workday after TO Execution | Distribution D | CUI | Monthly, as  requested |
|  | Training  Requirements  Definition \*\* | | Contractor Determined Format | Draft 45 Calendar Days after TO Execution | Distribution D | CUI | One Time;  Updated  annually as  required |
|  | Training  Material \*\* | | Contractor Determined Format | Monthly, on 5th workday after TO Execution | Distribution D | CUI | Monthly, as  required |
|  | Training  Feedback Forms \* | | Contractor Determined Format | Monthly, on 5th workday after TO Execution | Distribution D | CUI | Monthly, as  required |
|  | *[Insert Deliverable Title & Indicate level of responsibility based on ------]* | | *[Identify Format Type that* |  |  |  |  |
|  | *Add rows as needed* | |  |  |  |  |  |
| Symbol: | | Definition: | | | | | |
| \* | | 50% Government responsibility and 50% contractor responsibility | | | | | |
| \*\* | | 100% Contractor responsibility | | | | | |
| † | | These artifacts are built upon the packages submitted as part of the vendor's DoD PA | | | | | |

## Task 10 – Engineering Support

This section outlines requirements for technical/engineering support services. Support services may be provided to the DEOS Program Management Office (PMO) directly, or to DEOS customers. The contractor shall provide the full range of engineering support necessary to incorporate new/future technologies into the DEOS

service/baseline after initial deployment and must have expertise in both traditional IT infrastructure and cloud computing. The contractor shall provide comprehensive technical/engineering support services to include design, implementation, modification, and sustainment of DEOS projects and work activities. The scope includes any

future work efforts for both United States Territories and Possessions, as well as locations outside of the United States Territories and Possessions, NIPRNet and SIPRNet environments.

#### Subtask 1 – Systems Engineering

The contractor shall employ disciplined systems engineering processes including, but not limited to, requirements development, technical management and control, and system/software design and architecture. In addition, the contractor shall implement system engineering best practices associated with risk management, configuration management, data management, test and evaluation (T&E), and verification and validation (V&V) throughout the period of performance of the task orders.

#### Subtask 2 – Architecture and Service/System Design Engineering

The contractor shall support the design and development of systems and applications and their integration into the overarching enterprise DoD architecture. The contractor shall provide all required design and development documents, and supporting architectural documentation in compliance with Department of Defense Architectural Framework (DoDAF) Enterprise Architecture guidance, or other frameworks as identified in the task orders.

#### Subtask 3 – Network Engineering

The contractor shall support routing and switching analysis of enterprise-wide and large-scale networking infrastructure (CAN, MAN, WAN), to include, but not limited to, analyzing circuits, troubleshooting routing protocol configurations, making route optimization recommendations, highlighting traffic congestion points, and ensuring quality of service policies are properly configured. The contractor shall ensure network components are running the required hardware and software approved by the government, and validates network systems and transport layers are in compliance with industry standards and protocols. The contractor shall evaluate network problems, workflows, usage and trends to make organizational and planning recommendations, while developing appropriate corrective action.

#### Subtask 4 – Configuration Management Engineering

The contractor shall accomplish Configuration Management (CM) activities in accordance with DESMF best practices. CM activities include baseline identification, change control, status accounting, and auditing.

#### Subtask 5 – Test Engineering

The contractor shall develop dynamic provide a testing environments that will be used too support validate the CSO satisfies the government’s technical and operational requirements. C&A and functional testing . The contractor shall establish and maintain provided an integrated test lab shall support that is capable of supporting a full range of integration test activities for both the currently fielded system in as well as maintenance/modernization releases. The contractor shall support of the following test activities: in areas which include, but are not limited to, product testing (i.e., regression testing and new capability testing/evergreen); , operational scenarios testing (e.g., real world production environment simulation testing) considering system topology, y and concept of operations, disaster recovery, clustering, and load balancing; ), stress and longevity testing (e.g., load and throughput, speed of service, and duration); , interoperability testing (e.g., protocol translation, discrete systems communication); , security testing (e.g., VPN, Firewall, security configuration

#### Subtask 6 – Cybersecurity

The contractor shall assess the entire cybersecurity posture of the DEOS service and shall make recommendations to reduce support costs, and shall expose and remediate configuration and operational security issues before they affect the DEOS service. The contractor shall monitor the environment for security events and operational health. The contractor shall prevent the compromise of privileged account credentials from cyberattacks, promote credential hygiene and cybersecurity best practices, while ensuring systems/services comply with DoD cybersecurity requirements. The contractor shall coordinate with designated government personnel to ensure the DEOS services are available and optimized through security gateways.

#### Subtask 7 – Mobility Engineer

The contractor shall support the integration of the DEOS CSO and delivery of DEOS services to DoD approved mobile devices. The contractor shall support troubleshooting the DoD's Mobility Infrastructure (e.g., Mobile Device Management (MDMs), Gateways, security services and specific mobile PKI solutions) that are in direct support of DEOS services. The contractor shall ensure that all systems/services (e.g., email, web conferencing, file storage) are available via approved DoD mobile devices and that required DEOS mobile applications, tools, framework, and MAS are available for use across DoD.

#### Deliverables

The Government shall require the following documents as key deliverables for this task and sub-tasks. All deliverables listed below correspond with the key program milestones, activates, and deliverables listed in Attachment D. Any additional deliverables (i.e. not indicated below or in attachment D) maybe required by the Government based on the proposed technical/management approach and will be included at task order execution.

*[The contractor shall propose any additional deliverables based upon their technical and management approach that collectively provide sufficient evidence of satisfactory performance of activities required for this task and sub-tasks as applicable. Any additional deliverables included within the table below should also be included in key program milestone, activities, and deliverables list Attachment D]*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | DeliverableName | | Format | **Due Date** | **Distribution** | **Classification Marking** | **Frequency** |
|  | Engineering Artifacts (e.g., Network/System Diagrams) \*\* | | Contractor Determined Format | Within 10 business days after assignment | Distribution D  Distribution F | CUI | Monthly, as required |
|  | White Papers,  Information Papers and Decision  Papers \*\* | | Contractor Determined Format | Within 10 business days after assignment | Distribution D | CUI | Monthly, as required |
|  | Briefing Slides \*\* | | Contractor Determined Format | 30 Calendar Days after TO Execution | Distribution D | CUI | Weekly, as required |
|  | *[Insert Deliverable Title & Indicate level of responsibility based on ------]* | | *[Identify Format Type that* |  |  |  |  |
|  | *Add rows as needed* | |  |  |  |  |  |
| Symbol: | | Definition: | | | | | |
| \* | | 50% Government responsibility and 50% contractor responsibility | | | | | |
| \*\* | | 100% Contractor responsibility | | | | | |
| † | | These artifacts are built upon the packages submitted as part of the vendor's DoD PA | | | | | |

## Task 11 – Contract and Task Order Management

Provide all services necessary to manage and oversee all aspects of the contract and task order(s). Use key

performance parameters to monitor work performance, measure results, and ensure delivery of contracted product deliverables and solutions support management and decision-making and facilitate communications. Identify risks, resolve problems and verify effectiveness of corrective actions. Institute and maintain a process that ensures problems and action items discussed with the Government are tracked through resolution and shall provide timely status reporting. Results of contractor actions taken to improve performance shall be tracked, and lessons learned incorporated into applicable processes. Establish and maintain a documented set of disciplined, mature, and

continuously improving processes for administering all contract and task order efforts with an emphasis on

cost-efficiency, schedule, performance, responsiveness, and consistently high-quality delivery. The contractor shall provide a Monthly Service Utilization, Capacity, Outage and Upgrade Status and Forecast Report and

resources (i.e., personnel) required for closeout operations prior to contract completion.

**Deliverables:**

The Government shall require the following documents as key deliverables for this task and sub-tasks. All deliverables listed below correspond with the key program milestones, activates, and deliverables listed in Attachment D. Any additional deliverables (i.e. not indicated below or in attachment D) maybe required by the Government based on the proposed technical/management approach and will be included at task order execution.

*[The contractor shall propose any additional deliverables based upon their technical and management approach that collectively provide sufficient evidence of satisfactory performance of activities required for this task and sub-tasks as applicable. Any additional deliverables included within the table below should also be included in key program milestone, activities, and deliverables list Attachment D]*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Deliverable Title | | Format | **Due Date** | **Distribution** | **Classification Marking** | **Frequency** |
|  | Contractor Project Management Plan (CPMP) | | Contractor Determined Format | 15 Calendar Days after TO Execution | Distribution D  Distribution F | CUI | One Time; updated as required |
|  | Work Breakdown Schedule (WBS) | | Contractor Determined Format | Monthly, on 5th workday after TO Execution | Distribution D  Distribution F | CUI | Monthly, as  required |
|  | Integrated Master Schedule (IMS) | | Contractor Determined Format | 30 Calendar Days after TO Execution | Distribution D  Distribution F | CUI | Monthly, as  required |
|  | Task Order Status and Progress Report | | Contractor  Determined  Format | Monthly | Distribution D  Distribution F | CUI | Monthly, as  required |
|  | Subcontractor  Management Plan | | Contractor  Determined  Format | 30 Calendar Days  after Contract Award | Distribution D  Distribution F | CUI | One Time;  Updated  annually as  required |
|  | Kick-Off Meeting | | Contractor  Determined  Format | At the Task Order level within 15 days after task order award or unless  otherwise specified in the order | Distribution D | CUI | As required based on Task Order  execution |
|  | Quarterly Program Reviews | | Contractor  Determined  Format | For each Task Order, or unless otherwise specified in the Task Order. | Distribution D  Distribution F | CUI | As required based on Task Order  execution |
|  | Personnel Manpower Report | | Contractor  Determined  Format | Annually listing all personnel under each Task Order. | Distribution D  Distribution F | CUI | Annually, as  required |
|  | Contract Status Report | | Contractor  Determined  Format | Quarterly; unless otherwise specified by the Procuring Contracting Officer or Contracting  Officer Representative. | Distribution D  Distribution F | CUI | Quarterly, as  required |
|  | Post Award Task Order Meetings/Conferences | | Contractor  Determined  Format | Within five business days after conclusion of the meetings/conferences | Distribution D | CUI | As required |
|  | Briefing Slides | | Contractor Determined Format | 30 Calendar Days after TO Execution | Distribution D |  | Weekly, as  required |
|  | *[Insert Deliverable Title & Indicate level of responsibility based on ------]* | | *[Identify Format Type that* |  |  |  |  |
|  | *Add rows as needed* | |  |  |  |  |  |
| Symbol: | | Definition: | | | | | |
| \* | | 50% Government responsibility and 50% contractor responsibility | | | | | |
| \*\* | | 100% Contractor responsibility | | | | | |
| † | | These artifacts are built upon the packages submitted as part of the vendor's DoD PA | | | | | |

# Performance Standards

Performance Standards define the level of service required under the contract and subsequent task orders to successfully meet the performance objectives. Performance standards are the benchmark against which actual performance is measured. The Quality Assurance Surveillance Plan (QASP) defines all performance standards required under performance of the DEOS contract. The Contractor can be held accountable for meeting any or all of the performance standards identified in Appendix A of the QASP. Performance standards to be met during contract performance will be identified in each Task Order issued under the DEOS contract. The Government will determine performance standards to be monitored and perform surveillance as described in section 5 of the QASP to determine if the Contractor exceeds, meets, or does not meet the defined performance standards.

The Performance Standards Summary Matrix (Appendix A of the QASP) defines performance standards to which the Contractor must comply, as well as the methods that will be used to measure the quality of services provided under this contract. The Government will compare Contractor performance to the Acceptable Quality Level (AQL).

*[The Offeror may propose additional AQLs with their QASP that the Government has not indicated within Appendix A. However, at a minimum, all of the AQLs listed in Appendix A of Attachment 5, shall be included and addressed within the QASP. Based upon the proposed technical and management solution, the Offeror shall provide any additional performance standards, measures and values, comparable to or better than industry best practices, that enable the Government to verify satisfactory performance of each proposed task as applicable.]*

# Incentives

The identification of incentives (both positive and negative) will be addressed in each task order and reported in the Contractor Performance Assessment Reporting System (CPARS). In general, positive incentives may be used to reward significantly outstanding performance on a task order. Significantly, outstanding performance may

include employing process improvements and increased efficiencies, which result in significant cost savings for the Government, without compromising the quality of services or products provided. Adversely, negative

incentives may be utilized to penalize substandard or unacceptable quality of services or products in performance of the task order. The contractor is incentivized to earn favorable Government reviews to support continuation of DISA requirements and support contract awards with other Government agencies seeking DISA’s input on the contractor’s past performance.

# Place of Performance

Specific work location will be determined at the TO level. Work may be performed on-site, at all United States territories and possessions and Non-United States territories and possessions Government facilities or at the

contractor’s facility, sub-contractor facility, supplier, or other designated locations (e.g., corporate, 3rd party, or subcontractor). The Government will, if required, further specify the Periodic Progress Meetings at the task order level. On-site spaces at Government facilities may be revoked at any time per Government requirements.

Places of Performance shall include the following, at a minimum and subject to change based on TO

requirements: Ft. Meade (DISA HQ), Scott AFB, Stuttgart, GE, Honolulu, HI, and Ogden. Performance may be required at any Department of Defense location, worldwide.

For any contractor/sub-contractor facility, supplier, or other designated locations (e.g., corporate, 3rd party, or subcontractor) that are used to performance or meet TO requirements, the contractor shall provide the

Government with the following detailed information:

* Facility Name
* Point of Contact
* Description of Services/Data Provide at the location
* Geographic Location and Address

Travel in and around the primary place of performance may be required throughout the period of performance. Additional travel within the United States territories and possessions and Locations outside of the United States territories and possessions may be required to support the requirements of this SOO.

## Alternate Place of Performance (Contingency Only)

As determined by the Contracting Officer’s Representative (COR), contractor employees may be required to work at an alternate place of performance (e.g., home, the contractor's facility, or another approved activity within the local travel area) in cases of unforeseen conditions or contingencies (e.g., pandemic conditions, exercises, Government closure due to inclement weather, etc.). Non-emergency/non-essential contractors should not report to a closed Government facility. To the extent possible, the contractor shall use best efforts to provide the same level of support as stated in this SOO. In the event the services are impacted, reduced, compromised, etc., the Contracting Officer (CO) or the contractor may request an equitable adjustment pursuant to the Changes clause of the contract.

# Period of Performance

The period of performance for the BPA will be a 5-year base ordering period and two 2 year option periods and one 1 year option period (i.e. for a maximum total of ten years) and the 6-month extension of services IAW FAR 52.217-8. Period of Performance for each TO will be specified at the TO level. TOs that are awarded prior to the ordering period expiration can continue performance for a period not to exceed one year following the expiration of the ordering period. As directed by the COR, the contractor shall continue performance in emergency or mission essential conditions. Additionally, the contractor may be required to account for the whereabouts of their personnel should this information be requested by the COR.

# Security Requirements

This section shall be considered a supplement to Block 13 of the Government provided DD Form 254, Contract Classification Specification. The following security requirements shall apply to this effort. All contractor personnel shall possess, obtain, and maintain during the life of the contract the required security clearance over the life of the contract IAW DD Form 254, Contract Security Classification Specification. Contractor personnel shall comply with all applicable security and safety regulations, guidance, and procedures, including local, referenced in the requirement and in effect at the work sites.

Per the FedRAMP supplemental guidance for PS-3, found in the *FedRAMP Control Specific Contract Clauses v2*, June 6, 2014 document71, an agency must stipulate, “IAW OPM and OMB requirements”, the type of background investigation required for CSP personnel having access to or who can gain access to information. For DoD, the minimum designations are defined by level as follows:

***Impact Levels 5:*** CSP personnel supporting Level 5 cloud service offerings will meet the personnel security requirements and undergo background checks as defined in OPM policy IAW the FedRAMP Moderate baseline, the FedRAMP+ CEs related to personnel security, and DoD personnel security policies. As such the minimum background investigation required for CSP personnel having access to Level 4 and 5 information based on a “critical-sensitive” (e.g., DoD’s ADP-1) position designation, is a Single Scope Background Investigation (SSBI) or a Background Investigation (BI) for a “high risk” position designation. The minimum background investigation required for CSP personnel having access to Level 4 and 5 information based on a “noncritical-sensitive” (e.g., DoD’s ADP-2) is a National Agency Check with Law and Credit (NACLC) (for “noncritical-sensitive” contractors), or a Moderate Risk Background Investigation (MBI) for a “moderate risk” position designation.

***Impact Level 6:*** In accordance with PS-3(1), invoked by the CNSSI 1253 Classified Information Overlay, personnel having access to a secure room, the infrastructure supporting classified processing, or handling classified information, in addition to meeting the public trust position suitability/investigation requirements (e.g., a favorably adjudicated SSBI for a system administrator in a DoD ADP-1 position) must have a security clearance at the appropriate level. Systems and network administrators (i.e., privileged users), while typically not approved to handle classified information for need-to-know reasons, are considered to have access to classified information through their duties. Therefore these individuals require a clearance at the appropriate level for the classified information stored, processed, or transmitted.

**References**

1. DISA Form 786, DISA Statement of Information System Use and Acknowledgement of User

Responsibilities

1. DISA Policy Letter, Unauthorized Connections to Network Devices, 11 September 2013
2. DISAI 240-110-8, Information Security
3. DISAI 240-110-36, Personnel Security
4. DISAI 240-110-38, Industrial Security
5. DISA Instruction 630-230-19, Cybersecurity
6. DoDM 5200.01, Vol 1-4 Information Security Program, 24 February 2012
7. DOD 5200.2-R, DoD Personnel Security Program
8. DOD 5220.22-M, National Industrial Security Program Operating Manual, February 2006 Incorporating Change 02 May 2016
9. DOD 5220.22-R, Industrial Security Regulation
10. DoDM 5105.21 Sensitive Compartmented Information (SCI) Administrative Security Manual:

Administration of Information and Information Systems Security

## Facility Security Clearance

The work to be performed under this contract/order is up to the Top Secret level and will require Sensitive Compartmented Information (SCI) access eligibility for some personnel. Therefore the company must have an interim or final Top Secret Facility Clearance from the Defense Security Service Facility Clearance Branch.

## Security Clearance and Information Technology (IT) Level

All personnel performing on or supporting a DISA contract/order in any way will be U.S. citizens. The personnel security requirements for this contract/order cover the individuals supporting the Task Areas delineated in the table below. Contractor personnel must possess the interim or final security clearance and interim or final IT-level eligibility delineated in the table below when performance starts. In addition, if the Government sponsors a position at a certain clearance level, the Contractor is expected to maintain that position at the same clearance level.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SOO Task #** | **Clearance Level** | **IT Level Access** | **Level of Classified Access** | **Justification for Access to Classified** |
| 4.1 | Final Secret | Final IT-I | SCI | Provide a commercial service that is deployed in a DoD facility with a service that meets Impact Level 5 in accordance with DoD CCSRG requirements and that is geographically dispersed. At this time, we estimate that 15% of all personnel working in these areas will require SCI clearances. |
| 4.2 | Final Secret | Final IT-I | SCI | Provide a commercial service that is deployed in a DoD facility with a service that meets Impact Level 6 in accordance with DoD CCSRG requirements and that is geographically dispersed. At this time, we estimate that 15% of all personnel working in these areas will require SCI clearances. |
| 4.3 | Final Secret | Final IT-I | SCI | Provide a Denied, Disconnected, Intermittent, Limited Bandwidth (D-DIL) Environment in according with the DoD CCSRG for Impact Levels 5&6. At this time, we estimate that 15% of all personnel working in these areas will require SCI clearances. |
| 4.10 | Final Secret | Final IT-I | SCI | Provide technical/engineering support services including design, implementation, modification, and sustainment for both United States Territories and Possessions, as well as locations outside of the United States Territories and Possessions, NIPRNet (Impact Level 5) and SIPRNet (Impact Level 6) environments in according with the DoD CCSRG. At this time, we estimate that 15% of all personnel working in these areas will require SCI clearances. |

### Security Requirements for Top Secret or Top Secret/SCI Access

Security requirements for Top Secret or Top Secret/SCI access will be identified at the individual task order level. Individuals supporting PWS Tasks / Subtasks that require(s) an interim or final Top Secret security clearance and an interim or a final IT-I (privileged level system access) will, immediately upon hire, require Sensitive Compartmented Information (SCI) access eligibility adjudicated by the Defense Intelligence Agency or other federal adjudications facility to perform their duties. SCI processing for SCI eligibility will be coordinated with the supporting Government Security Manager and will begin immediately upon start of duty performance under this contract/order. All SCI work under this contract/ order will be monitored by the POC(s) identified at the individual task order level.

## Investigation Requirements

All personnel requiring SCI, Top Secret or IT-I access under this contract/order shall undergo a favorably

adjudicated Tier 5 investigation (formerly known as a Single Scope Background Investigation (SSBI)) as a minimum requirement. The Tier 5 will be maintained current within 5-years and requests for Tier 5 reinvestigation (T5R) (formally known as a Single Scope Background Period Reinvestigation (SBPR) or Phased Periodic Reinvestigation (PPR)) will be initiated prior to the 5-year anniversary date of the previous Tier 5.

### Secret or IT-II Access

All personnel requiring Secret or IT-II access under this contract/order shall undergo a favorably adjudicated Tier 3 (T3) investigation (formerly known as a National Agency Check, Local Agency Check and Credit Check or Access National Agency Check and Inquiries) as a minimum investigation. The T3 investigation will be maintained current within 10-years and requests for Secret Periodic Reinvestigations will be initiated by submitting a Tier 3R investigation request prior to the 10-year anniversary date of the previous Tier 3 investigation.

Contractor personnel that do not meet the investigation requirements for Secret IT-I access may be granted such access by the DISA Personnel Security Office (DISA PSO) provided there is no disqualifying information within the adjudicative guidelines that cannot be mitigated. The DISA PSO will request the contractor personnel complete an Electronic Questionnaire for Investigation Processing (e-QIP). The DISA PSO will review the e-QIP and if there is no disqualifying information, the individual may be eligible for interim Secret IT-I access. Once favorable results are returned from the Federal Bureau Investigation (FBI) name and fingerprint check, the National Agency Check portion of the investigation is completed favorable, DISA PSO may grant the interim Secret IT-I provided all other conditions are met. Contract personnel found ineligible for interim Secret IT-I access will not be allowed to support a DISA contract requiring Secret IT-I access and must wait for final favorable adjudications by the appropriate adjudication facility.

## Adjudication for Secret IT-I Access

Favorable Adjudication of any previous T5, T5R, SSBI, SBPR or PPR by any of the DoD Central Adjudication Facility or other federal adjudications facilities within a five-year period will be automatically accepted for final Secret IT-I access.

### Interim Secret IT-I Authorization

Prior to granting interim Secret IT-I authorization, the supporting security manager will forward a written request for interim Secret IT-I authorization to DISA PSO for approval. The request for SSBI (e-QIP, FBI name and fingerprint check) must be submitted by DISA PSO to the Office of Personnel Management (OPM).

## Visit Authorization Letters (VAL)

Visit requests shall be processed and verified through the Joint Personnel Adjudication System (JPAS) to SMO DKABAA10 and SMO DKADAL. JPAS visits for contracts/orders are identified as “Other” or “TAD/TDY” and will include the contract/order number and ADP/IT-Access level of the contract/order in the Additional Information section. Contractors that do not have access to JPAS may submit visit authorizations by e-mail in a password protected PDF to the Contracting Office Representative (COR) or Alternate COR specified in PWS Section 1.0.

If JPAS is not available, the VAL must contain the following information on company letterhead:

* Company name, address, telephone number, assigned CAGE Code, facility security clearance
* CAGE Code
* Contract / Order Number
* Name, SSN, date and place of birth, and citizenship of the employee intending to visit
* Certification of personnel security clearance and any special access authorizations required for the visit (type of investigation & date, adjudication date & agency, and IT access level)
* Name of COR / Alt COR
* Dates or period the VAL is to be valid

## Security Contacts

DISA Security Personnel can be contacted for Industrial or Personnel Security related issues at (301) 225-1235 or via mail at:

|  |  |
| --- | --- |
| Defense Information Systems Agency  **ATTN:**  MP61, Industrial Security  Command Building  6910 Cooper Ave.  Fort Meade, MD 20755-7088 | Defense Information Systems Agency  **ATTN:** MP62, Personnel Security  Command Building  6910 Cooper Ave.  Fort Meade, MD 20755-7088 |

For Center or Directorate-specific security related matters, contact the Directorate or Center Security Manager at:

|  |  |
| --- | --- |
| Defense Information Systems Agency  **ATTN:**  Abigalee Conrad | **Comm:** (301) 255-1262  **Email:**  [Disa.meade.bd.mbx.sd-security-managers@mail.mil](mailto:Disa.meade.bd.mbx.sd-security-managers@mail.mil) |

# Information Security and Other Miscellaneous Requirements

## Entry/Exit Security Controls

Contractor personnel shall comply with all local security requirements including entry and exit control for personnel and property at the Government facility.

## Periodic Safety and Security Training

Contractor employees shall be required to comply with all Government security regulations and requirements. Initial and periodic safety and security training and briefings will be provided by Government security personnel. Failure to comply with Government security regulations and requirements shall require the company to provide the Government with a written remediation/corrective action plan; furthermore, failure to comply with such requirements can be cause for removal and the contractor will not be able to provide service on this contract/order.

## Contractor with incidents in JPAS

Contractor employees with an incident report in JPAS who have had their access to classified suspended will not be permitted to provide to fill positions requiring access to classified information on a DISA contract/order.

## Divulging Classified or Unclassified

The contractor shall not divulge any information, classified or unclassified, about DoD files, data processing activities or functions, user identifications, passwords, or any other knowledge that may be gained, to anyone who is not authorized to have access to such information. The contractor shall observe and comply with the security provisions in effect at the DoD facility. Identification shall be worn and displayed at all times as required.

## Removal of Contractor Personnel

The Government retains the right to request removal of contractor personnel regardless of prior clearance or adjudication status, whose actions, while assigned to this contract, clearly conflict with the interest of the Government.

## Information Handling

Contractor personnel will generate or handle documents that contain For Official Use Only (FOUO) information at the contractor and/or Government facility. Contractor shall have access to, generate, and handle classified

material only at the location(s) listed in the place of performance section of this document. All contractor

deliverables shall be marked IAW DoDM 5200.1, Vol 3, Vol. 4, Information Security, DoD 5400.7-R, FOIA

Program, unless otherwise directed by the Government. The contractor shall comply with the provisions of the DoD Industrial Security Manual for handling classified material and producing deliverables. The contractor shall comply with DISA Instruction 630-230-19.

## Government-Furnished Property (GFP)/ Government Furnished-Equipment (GFE)/Government Furnished Information (GFI)

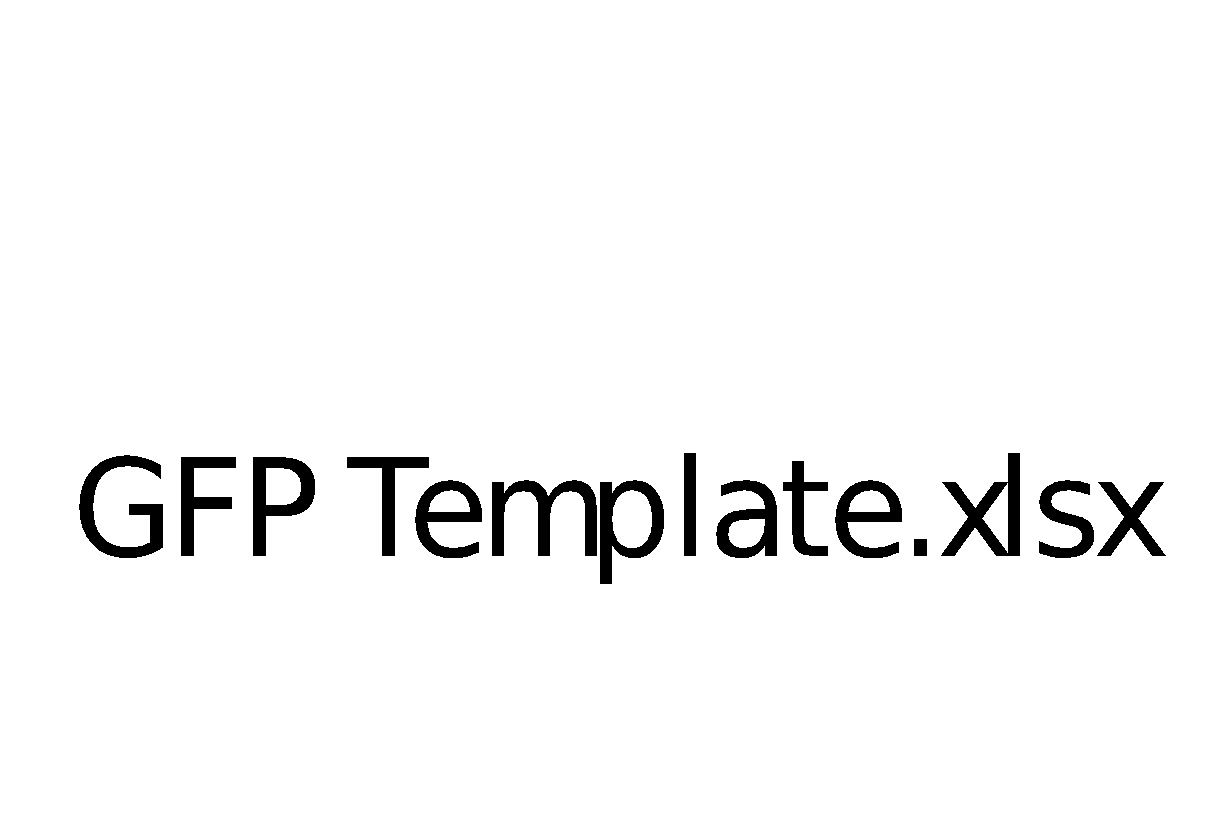
The GFP provided to the contractor may include, but is not limited to, laptops and mobile devices to perform the services needed under this contract/order. The contractor shall manage GFP at the TO level in accordance with Federal Acquisition Regulation (FAR) Part 45, Defense FAR Supplement (DFARS) Part 245 and associated clauses incorporated in this contract. The contractor shall include a complete list of all GFP for each TO within the contractor's Monthly Status Report for verification by the COR and/or Property Administrator. Each list shall include the Make, Model, Serial Number, End Warranty Date, and Bar Code of every laptop and provide similar detailed information for each other piece of GFP. GFI will include the following: a roster of designated key

personnel and authorized POCs; security procedures; manuals; and operating procedures.

DoD Instruction 4161.02 provides over all GFP guidance. FAR 52.245-1 establishes the foundation GFP requirements. The following 5 DFARS clauses compel accurate management and reporting of GFP by contractors:

* DFARS 252.211-7007: Reporting of Government-Furnished Property. Provides definitions of GFP-related terms and requirements of reporting GFP to the IUID Registry; Includes data to report to the IUID Registry and reporting procedures
* DFARS 252.245-7001: Tagging, Labeling, and Marking of Government-Furnished Property. Establishes definition of serially-managed items and requirement of tagging, labeling and marking of GFP
* DFARS 252.245-7002: Reporting Loss of Government Property. Defines loss of Government Property; Provides Contractors with procedures on how to report the loss of Government Property
* DFARS 252.245-7003: Contractor Property Management System Administration. Provides guidance on what is an acceptable Contractor system or systems for managing and controlling Government Property
* DFARS 252.245-7004 Reporting, Reutilization, and Disposal. Outlines procedures on inventory disposal schedules; sales of surplus property proceeds; demilitarization, mutilation, and destruction; contractor inventory; and disposal of scrap.

Accountability of GFP, GFE, and GFI requirements will be determined at the task order level. If applicable, the contractor shall submit the attached GFP template (see below) in addition to complying with all requirements of DFARS clauses listed above.



# Other Pertinent Information or Special Considerations

## Identification of Possible Follow-on Work: Not applicable (N/A)

## Identification of Potential Organizational Conflicts of Interest (OCI)

The contractor employees and subcontractor or other supporting organization employees shall refrain from using Government data for any purpose other than expressly stated in the requirements of the contract. The contractor shall identify any potential or actual organizational conflicts of interest (OCI) per Defense Acquisition

Regulations System (DARS) Clause 52.209-9000. An “organizational OCI” is a situation where because of other relationships or activities a person/company is unable or potentially unable to render impartial assistance or

advice to the Government, or cannot objectively perform contract work, or has had access to information giving it an unfair competitive advantage.OCI is defined as:

* A Government solicitation/contract requires a contractor to exercise judgment to assist the Government in a matter (such as in drafting specifications or assessing another contractor’ proposal or performance) and the contractor or its affiliates have financial or other interests at stake in the matter, so that a reasonable person might have concern that when performing work under the contract, the contractor may be

improperly influenced by its own interests rather than the best interests of the Government; or

* A contractor could have an unfair competitive advantage in an acquisition as a result of having performed work on a Government contract, under circumstances such as those described in paragraph (1) of this

definition, which put the contractor in a position to influence the acquisition; or

* Nonpublic information, as used in this section, means any Government or third-party information that: (1) Is exempt from disclosure under the [FOIA](http://www.westlaw.com/Find/Default.wl?rs=dfal.0&vr=2.0&DB=1000546&DocName=5USCAS552&FindType=L) or otherwise protected from disclosure by statute, Executive order, or regulation; or (2) Has not been disseminated to the general public, and the Government has not yet determined whether the information can or will be made available to the public.

The contractor shall provide the Government an OCI Plan for purposes of identifying, mitigating, or avoiding OCIs IAW FAR Subpart 9.5. Contractors shall identify any possible OCI issues and provide a mitigation plan for them and for any other OCI issues that may subsequently arise during performance of the contract. Contractor analysis should include, but is not necessarily limited to, financial interests, and any contract work that involves the review of goods or services produced by industry competitors. Disqualification may be required for individual task orders if performance of work under this contract or other contracts results in an OCI that cannot be

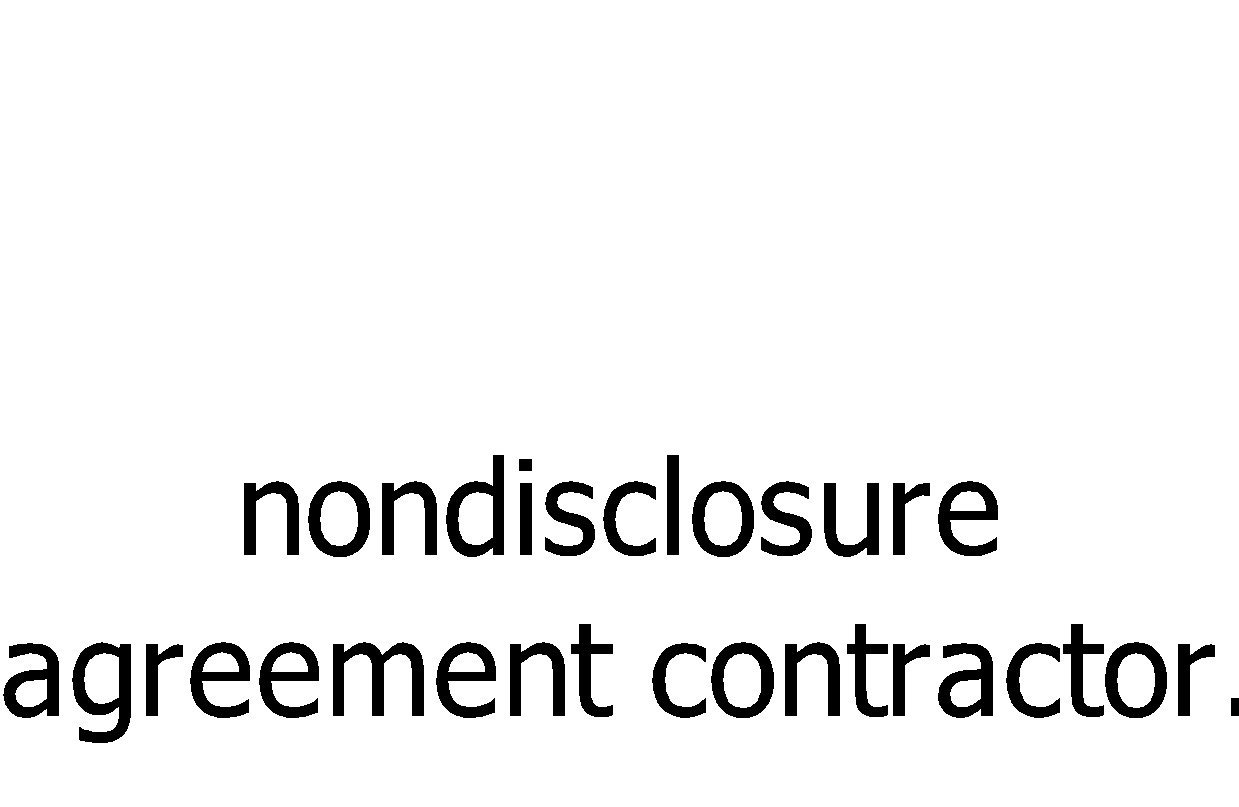
adequately mitigated, and such determinations will be made by the OCI on a case-by-case basis.

## Identification of Non-Disclosure Agreement (NDA) Requirements

The contractor employees and subcontractor(s) or other supporting organization employees with access to

Government data and other Government confidential information shall sign DISA provided non-disclosure

agreements (NDAs) that legally prevent any employee from disclosing non-public Government information. All contractors must execute a DISA-provided contractor NDA for all services contracts regardless of award amount. The NDA must be signed within one week of contract/task order award. The DISA contractor is responsible for obtaining and maintaining NDAs for each contractor employee assigned to the contract/task order. The NDA is attached to this SOO for your convenience.

**

The contractor is responsible for identifying that all personnel, to include any new personnel on the contract, have executed the DISA-provided NDA and the NDA is current as of the date of the monthly status report.

**Deliverable:** The contractor shall provide a Monthly Status Report (contractor-determined format) to the KOs and CORs 30 Calendar Days after Award and by no later than the 5th business day of every month.

## Packaging, Packing and Shipping Instructions

Packaging, packing and shipping instructions will be determined at the task order level.

## Inspection and Acceptance Criteria

Inspection and acceptance will be conducted by the designated COR(s) at the task order-level. Additional

information related to the inspection and acceptance criteria that will be used based on task order requirements is outlined in Section E of the solicitation.

## Key Personnel Requirements

The following positions, or comparable labor categories as proposed by the Offeror, are deemed Key Personnel; however, the Government reserves the right to designate additional individuals and labor categories as Key Personnel based upon review of the Offeror’s proposal in accordance with DARS 52.237-9000.

|  |  |
| --- | --- |
| **Name** | **Position/Labor Category** |
| *[Insert Name of Key Personnel]* | Project Lead/Manager |
| *[Insert Name of Key Personnel]* | Migration Manager |
| *[Insert Name of Key Personnel]* | Operation Manager |
| *[Insert Name of Key Personnel]* | Enterprise Architect |
| *[Insert Name of Key Personnel]* | Directory Services Lead Engineer |
| *[Insert Name of Key Personnel]* | Master Scheduler |
| *[Insert Name of Key Personnel]* | Communication Manager |
| *[Insert Name of Key Personnel]* | Configuration Specialist/Manager |
| *[Insert Name of Key Personnel]* | Cybersecurity - Systems Engineer |

# Cyber Threat Security Plan

In conjunction with the DFARS Subpart 204.73, Safeguarding Unclassified Controlled Technical Information, DFARS Clause 252.204-7012, Safeguarding unclassified controlled technical information, and DoD, DISA, NIST, and other Federal mandated regulations, instructions, procedures, and laws, the contractor shall develop, submit, and implement upon approval a Cyber Threat Security Plan.

This plan shall be consistent with and further detail the approach contained in the contractor proposal that resulted in the award of this contract and in compliance with the requirements stated in the clause mentioned under this task. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall contain the following:

* **Vulnerability Management:** Evaluate network components, security procedures, and processes for

potential exploitation from attack.

* **Cyber Threat Intelligence:** Provide policy enforcement and end-point protection against unwarranted attacks on the network.
* **Analytics Monitoring:** Provide scalable analytics solution capable of combining potential risk indicators and developing leads.
* **Mitigation and Response:** Provide the process on how the threat will be mitigated and responded to upon discovery.
* **Lessons Learned and Action Strategy:** Provide lessons learned and an action plan that will help all

interested parties avoid repeated and similar attacks.

* **Subcontractors:** explain how your subcontractors will be required to implement this requirement within their processes in support of this task.
* **Cybersecurity Testing Approach:** Provide support to the Government DT&E, OT&E and IOP
* activities/events, to include cybersecurity testing in accordance with the DoD Cybersecurity T&E

guidebook process.

**Deliverable:** The CSP shall provide the Government with a Cyber Threat Security Plan thirty (30) business days after contract award to the BPA Contracting Officer and COR for acceptance. The BPA Contracting Officer and COR have ten (10) business days to provide written acceptance or feedback to the contractor. If no written acceptance is received within the ten (10) business days, then the contractor can consider the plan accepted. If the contractor receives feedback within the ten (10) working days, then the contractor has ten (10) business days to provide the BPA Contracting Officer and COR an updated plan based on comments provided by the Government.

Annually, on the anniversary date of acceptance of the Cyber Threat Security Plan, the contractor shall submit verification to the BPA Contracting Officer and COR that the Plan remains valid or update as required.

# Data Breach/Loss/Privacy Impact Management

The contractor shall provide the Government with a Data Loss Prevention and Countermeasures Management (DLPCM) Plan (contractor-determined format) for handling any breach or data loss, which includes the

requirement to notify the DISA of such breach within 60 minutes of detection. In addition, the contractor shall support, document and report the conduct of a Privacy Impact Assessment (PIA) for all IT systems utilized to the deliver the service. The purpose of the PIA is to analyze how information in identifiable form is handled: to

ensure that its handling conforms to applicable legal, regulatory, and policy requirements for privacy; to

determine the risks and effects of collecting, maintaining, and disseminating such information in an electronic

information system; and to examine and evaluate protections and alternative processes for handling such

information to mitigate potential privacy risks. To assist in completing the PIA, the contractor shall provide DISA with all relevant information and data in the form and quality required for completion.

**Deliverable:** The CSP shall provide the Government with a DLPCM Plan thirty (30) business days after contract award to the BPA Contracting Officer and COR for acceptance. The BPA Contracting Officer and COR have ten (10) business days to provide written acceptance or feedback to the contractor. If no written acceptance is received within the ten (10) business days, then the contractor can consider the plan accepted. If the contractor receives feedback within the ten (10) working days, then the contractor has ten (10) business days to provide the BPA Contracting Officer and COR an updated plan based on comments provided by the Government.

Annually, on the anniversary date of acceptance of the DLPCM Plan, the contractor shall submit verification to the BPA Contracting Officer and COR that the plan remains valid.

# Transition and Decommission

The contractor shall provide a Transition and Decommissioning Plan (contractor-determined format) that outlines the necessary support for a seamless uninterrupted transition of work at the beginning and ending of this ID/IQ contract as well as the follow-on task orders. An organized transition between the contractor and an incumbent or successor contractor is necessary to assure minimum disruption to vital Government business. The contractor shall develop a decommissioning process that includes the following steps: notification; submittal and review of the Post-Shutdown Decommissioning Activities Report (PSDAR); submittal and review of the license termination plan (LTP); implementation of the LTP; and completion of decommissioning.

At contract end, the contractor shall return all data to the Government. Contractor shall ensure that no residual DoD data exists on all storage devices decommissioned and disposed of, reused in an environment not governed by an agreement between the contractor and DoD, or transferred to a third party; as required by the FedRAMP selected security control MP-6. Refer to the DoD CC SRG, sections 5.8 and 5.9 for detailed information.

**Deliverable:** The CSP shall provide the Government with a Transition and Decommissioning Plan thirty (30) business days after contract award to the BPA Contracting Officer and COR for acceptance. The BPA Contracting Officer and COR have ten (10) business days to provide written acceptance or feedback to the contractor. If no written acceptance is received within the ten (10) business days, then the contractor can consider the plan accepted. If the contractor receives feedback within the ten (10) working days, then the contractor has ten (10) business days to provide the BPA Contracting Officer and COR an updated plan based on comments provided by the Government.

Annually, on the anniversary date of acceptance of the Cyber Threat Security Plan, the contractor shall submit verification to the BPA Contracting Officer and COR that the Plan remains valid or update as required.

# Supply Chain Risk Management (SCRM)

Section 5.18 of the DoD CC SRG outlined the Supply Chain Risk Management (SCRM) Plan requirements for this acquisition. The contractor will provide the Government with a copy of the SCRM plan that was submitted as part of their FedRAMP assessment package, which is updated annually. The plan should outline the supply chain assessment/management and component authenticity process and measures taken such that they are not acquiring system components and software that are counterfeit, unreliable, or contain malicious logic or code and

incorporating them into the CSO infrastructure or its management plane.

This contract and its associated delivery/task orders are subject to the Federal SCRM policies and regulations

including the Defense Federal Acquisition Regulation Supplement (DFARS) 252.239-7017 Notice of Supply Chain Risk, 252.239-7018 Supply Chain Risk, DoD Instruction 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, Section 806 of the FY2011 NDAA Requirements for Information

Relating to Supply Chain Risk, and internal DISA SCRM Processes and Procedures. The SCRM plan shall

describe the contractor’s use of system security engineering processes in specifying and designing a system that is protected against external threats and against hardware and software vulnerabilities.

**Deliverable:** The CSP shall provide the Government with a SCRUM Plan thirty (30) business days after contract award to the BPA Contracting Officer and COR for acceptance. The BPA Contracting Officer and COR have ten (10) business days to provide written acceptance or feedback to the contractor. If no written acceptance is received within the ten (10) business days, then the contractor can consider the plan accepted. If the contractor receives feedback within the ten (10) working days, then the contractor has ten (10) business days to provide the BPA Contracting Officer and COR an updated plan based on comments provided by the Government.

Annually, on the anniversary date of acceptance of the SCRM Plan, the contractor shall submit verification to the KO and COR that the plan remains valid or within five (5) business days whenever there is a change that affects one or more security controls as described in the Committee on National Security Systems Instruction (CNSSI) 1253 (companion publication to NIST Special Publications (SP)). At a minimum, the following events substantiate the need for an update: changes in company ownership, changes in senior company leadership, supplier changes, subcontractor changes, and ICT supply chain compromises.

# Section 508 Accessibility Standards

All Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 United States Code (U.S.C.) 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology

Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The CSP identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards.

The CSP shall maintain and retain full documentation of the measures taken to ensure compliance with the

applicable requirements, including records of any testing or demonstrations conducted. When the CSP is required (i.e., as requested bases by the Government) to perform testing to validate conformance to accessibility

requirements, the CSP shall provide a Supplemental Accessibility Conformance Report (SAR) that contains the following information:

* Accessibility test results based on the required test methods
* Documentation of features provided to help achieve accessibility and usability for people with disabilities.
* Documentation of core functions that cannot be accessed by persons with disabilities.
* Documentation on how to configure and install the product/service item to support accessibility and use with assistive technology.
* When a product/service is an authoring tool that generates content (including documents, reports, videos, multimedia productions, web content, etc.), provide information on how the product/service enables the creation of accessible electronic content that conforms to the Revised 508 Standards, including the range of accessible user interface elements the tool can create.
* Before final acceptance, the contractor shall provide a fully working demonstration of the completed product/service to demonstrate conformance to the agency’s accessibility requirements. The
* demonstration shall expose where such conformance is and is not achieved.

Before acceptance, the Government reserves the right to perform independent testing to validate the product/

service provided by the CSP conforms to the applicable Revised 508 Standards. The CSP must state tasks to meet section 508 accessibility in the PWS (Attachment 4) if the proposed CSO does not meet all of the 508 Standards.

**Deliverable:** The CSP shall use the GSA 508 Voluntary Product Accessibility Template (VPAT) and provide the Government with the completed thirty (30) business days after contract award to the BPA Contracting Officer and COR for acceptance. The BPA Contracting Officer and COR have ten (10) business days to provide written acceptance or feedback to the contractor. If no written acceptance is received within the ten (10) business days, then the contractor can consider the plan accepted. If the contractor receives feedback within the ten (10) working days, then the contractor has ten (10) business days to provide the BPA Contracting Officer and COR an updated plan based on comments provided by the Government.

Annually, on the anniversary date of acceptance of the VAPT, the contractor shall submit verification to the KO and COR that the VPAT remains valid or update as required. If the CSP offers more than one service (i.e., email, content management, etc.) the Government will require a separate VPAT for each product/service that is part of the proposed CSO. Before testing or whenever there is a change that affects the VPAT submitted at BPA award, the CSP shall provide an Accessibility Conformance Report (ACR) for each product/service that is

developed, updated, or re-configured. The ACR should be based on the VAPT Version 2.0 provided by the

Industry Technology Industry Council (ITIC).

1. A tenant is defined as a client or organization that owns and manages a specific instance of a cloud service. Each tenant is distinct and separate from other tenants in that it isolates customer data, prevents identity information from co-mingling (e.g., users and administrators of one tenant cannot accidentally or maliciously access data in another tenant) and has an account that provides unrestricted administrative access to features and functions of the instance. [↑](#footnote-ref-1)