**STATEMENT OF OBJECTIVES (SOO)**

**as of 16 April 2018**

|  |  |
| --- | --- |
| **Contract Number:** | **TBD** |
| **Task Order Number:** | **TBD** |
| **Contractor Name:** | ***TBD*** |
| **Tracking Number:** | **HC1047-18-F-4007** |

# Contract Title: Defense Enterprise Office Solutions (DEOS)

# Background

The Department of Defense (DoD) requires an integrated enterprise cloud service offering (CSO) for common communication, collaboration, and productivity capabilities that are mission-effective, efficient, more widely accessible, to 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 office productivity.

# Objectives

DEOS is a new procurement of a CSO that will support the Department’s move towards implementing capabilities for the Joint Information Environment (JIE) vision, improving trusted information sharing, and integration of virtual enterprise services into DoD strategic environments. 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 disparate DoD-wide legacy enterprise collaboration, voice/video, and productivity capabilities.

The DEOS CSO will be acquired by DISA through an unrestricted, competitively awarded single-award Indefinite Delivery/Indefinite Quantity (ID/IQ) Firm-Fixed Price (FFP) contract with a contractor who will provide a non-developmental, seamlessly integrated CSO. The contract period of performance will be a 5-year base ordering period and five 1-year options ordering period. The contract also 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. The anticipated initial task order issued against this ID/IQ could potentially include the current 1.8 million legacy United States territories and possession NIPRNet DEE user population.

# Scope

DEOS will provide the DoD with an integrated, interoperable, enterprise CSO to support approximately 3.15 million DoD consumers, standardize adoption, and enable cross-Department collaboration at local base/post/camp/station (B/P/C/S) levels to include 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, 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 some of the existing DoD supporting infrastructure, services, and major integration points that will reside primarily on-premises as part of the Government’s responsibility and which the Cloud Service Provider (CSP) must integrate with. These specific supporting infrastructure and services outline the DoD required integration points that the CSP will be responsible for ensuring interoperability and integration with. Additional, information related to the DoD supporting infrastructure and service requirements are outlined within section 4 of the Functional Requirements Document (FRD).

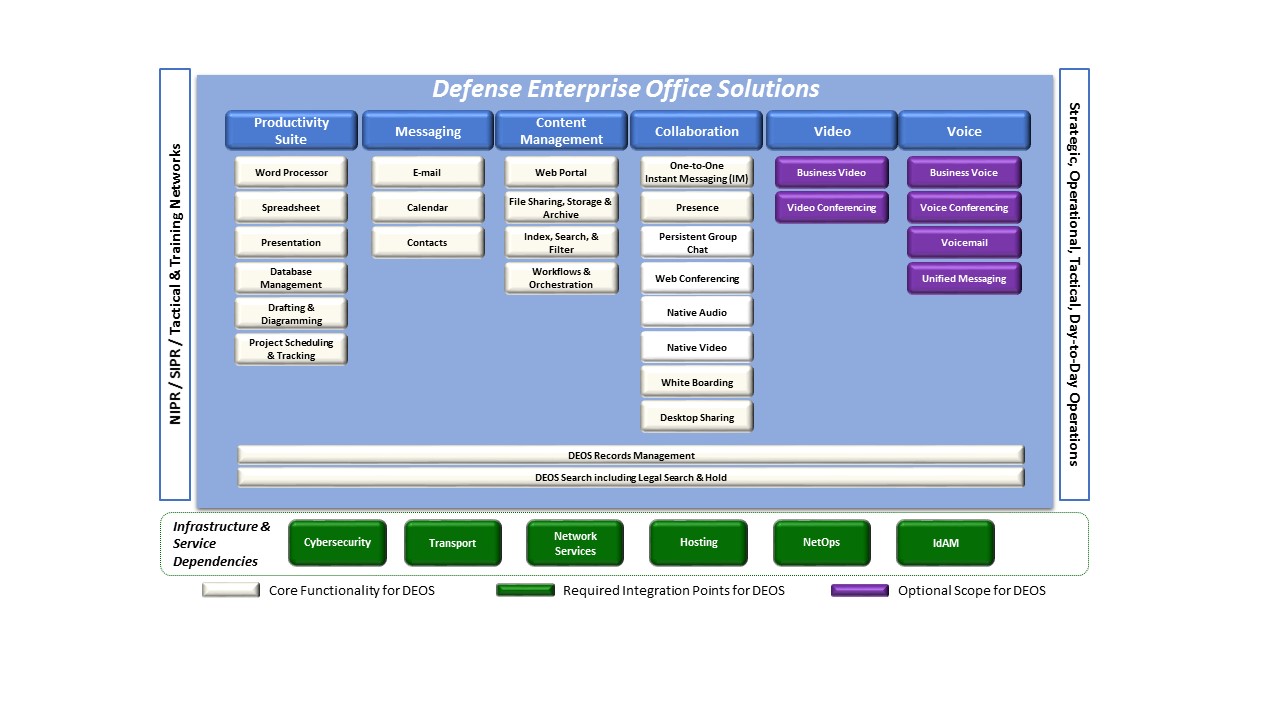


Figure 1 – DEOS Service Requirements

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 the United States territories and possessions NIPRNet and SIPRNet implementations, the Government will leverage commercially hosted facilities to meet the DEOS requirements. However, due to DoD data sovereignty requirements, locations outside of the United States territories and possessions the contractor will be required to implement a NIPRNet and SIPRNet CSO within a DoD data centers (e.g. Stuttgart, Wiesbaden, Capodichino).

For all implementation locations outside of the United States territories and possessions the contractor will be required to provide a stand-alone environment within a DoD data center that includes, the required infrastructure, hardware, software, and any other additional components required to implement, management, and maintain the CSO environments. The Government will provide and identify the DoD data center facilities based on the contractor proposed 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 (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 Objectives

The contractor shall propose performance tasks that fully adhere to the requirements of the solicitation and the DEOS FRD (Attachment 01), DoD Cloud Computing Security Requirements Guide (CC SRG), and DoD security control requirements to achieve and maintain Authorization to Operate (ATO), Provisional Authorization (PA) at Impact Level (IL) 5 (Controlled Unclassified Information) and IL 6 (Classified Information up to Secret) utilizing the Performance Work Statement (PWS) format (Attachment 4) provided as part of this solicitation.

The deliverables and performance standards based the proposed technical and management solution, shall incorporate the mandatory contract deliverables, the performance standards (section 6), Cyber Threat Security Plan (section 16), Supply Chain Risk Management (SCRM) requirements (section 19), and Section 508 Accessibility Standards (section 20) in the proposed PWS.

## Task 1 – NIPRNet Environment

The contractor shall deliver a cloud architecture and corresponding environment that supports a multiple tenant. The NIPRNet CSO shall include System Wide, Core Services (i.e. Email, IM/Chat, Web Conferencing, Native Audio, Native Video, Content Management, and Office Productivity), Record Management, and DoD Information Network (DoDIN) Protection requirements in accordance with (IAW) the FRD sections 2, 3, and 4.

Furthermore, the contractor shall be required to interface the CSO to the core integration points identified in the FRD section 7. Lastly, the contractor shall adhere to the performance objectives identified in the FRD section 9, and shall be required to perform testing activities/events (i.e. integration, acceptance, operational) IAW the FRD section 10, to verify the proper interoperability between the CSO and core integration points (FRD section 7).

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

Provide a geographically dispersed ***off-premises*** CSO within a DoD private/community hybrid cloud that meets IL 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 hybrid Cloud Service Offering (CSO) that is deployed in an DoD facility 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 the deliverables for this task and sub-tasks. The contractor shall incorporate these deliverables into the proposed PWS. In addition, 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.

| Deliverable Title | Format | **Due Date** | **Distribution** | **Frequency** |
| --- | --- | --- | --- | --- |
| Implementation Plan | Contractor  Determined Format | 30 Calendar Days after Award | Standard  Distribution\* | One Time Update annually as  required |
| Work Breakdown Schedule (WBS) | Contractor  Determined Format | Monthly, on 5th workday after TO Execution | Standard  Distribution\* | Monthly, as  Required |
| Integrated Master Schedule (IMS) | Contractor  Determined Format | 90 Calendar Days after TO  Execution | Standard  Distribution\* | Monthly, as  required |
| Architecture, DoDAF  Artifacts/Diagrams (i.e. AV, OV, SV, StdV, CV) | Contractor  Determined Format | 90 Calendar Days after TO  Execution | Standard  Distribution\* | One Time  Update annually as required |
| Interfaces, Ports & Protocols Baseline | Contractor  Determined Format | 90 Calendar Days after TO  Execution | Standard  Distribution\* | One Time  Update annually as required |
| Service Support Functions and  Integration Plan | Contractor  Determined Format | 30 Calendar Days after Contract Award | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Records  Management  Architecture/  Integration Plan | Contractor  Determined Format | 30 Calendar Days after TO  Execution | Standard  Distribution\* | One Time Update annually as  required |
| Cybersecurity  Monitoring Strategy | Contractor  Determined Format | 30 Calendar Days after Contract Award | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Transition/  Decommission Plan | Contractor  Determined Format | 60 Calendar Days after Contract Award | Standard  Distribution\* | One Time  Updated  annually as  required |
| Requirements  Management Plan / Traceability Matrix | Contractor  Determined Format | 30 Calendar Days after TO  Execution | Standard  Distribution\* | Weekly, as  required |
| Customer  Communication Plan | Contractor  Determined Format | 30 Calendar Days after TO  Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| White Papers,  Information Papers and Decision Papers | Contractor  Determined Format | 30 Calendar Days after TO  Execution | Standard  Distribution\* | Monthly, as  required |
| Briefing Slides | Contractor  Determined Format | 30 Calendar Days after TO  Execution | Standard  Distribution\* | Weekly, as  required |
| \* **Standard Distribution:**   1. 1 copy of the transmittal letter without the deliverable to the Contracting Officer shall be uploaded to <https://www.ditco.disa.mil/dcop/Public/ASP/dcop.asp>. 2. 1 copy of the transmittal letter with the deliverable to the Primary COR or Government designated repository. | | | | |

## Task 2 – SIPRNet Environment

The contractor shall deliver a cloud instance architecture and corresponding environment that supports multiple tenants. The SIPRNet CSO shall include System Wide, Core Services (i.e. Email, IM/Chat, Web Conferencing, Native Audio, Native Video, Content Management, and Office Productivity), and DoD DoDIN Protection requirements IAW the FRD sections 2, 3, and 4. Furthermore, the contractor shall be required to interface the CSO to the core integration points identified in the FRD section 7. Lastly, the contractor shall adhere to the performance objectives identified in the FRD section 9, and shall be required to perform testing activities/events (i.e. integration, acceptance, operational) IAW the FRD section 10, to verify the proper interoperability between the CSO and core integration points (FRD section 7).

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

Provide a geographically dispersed ***off-premises*** CSO within a DoD private/community hybrid cloud that meets IL 5 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 hybrid CSO that is deployed in an DoD facility 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 the deliverables for this task and sub-tasks. The contractor shall incorporate these deliverables into the proposed PWS. In addition, 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.

| Deliverable Title | Format | **Due Date** | **Distribution** | **Frequency** |
| --- | --- | --- | --- | --- |
| Implementation Plan | Contractor Determined Format | 30 Calendar Days after Award | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Work Breakdown Schedule (WBS) | Contractor Determined Format | Monthly, on 5th workday after TO Execution | Standard  Distribution\* | Monthly, as  required |
| Integrated Master Schedule (IMS) | Contractor Determined Format | 90 Calendar Days after TO Execution | Standard  Distribution\* | Monthly, as  required |
| Architecture, DoDAF  Artifacts/Diagrams (AV, OV, SV, StdV, CV) | Contractor Determined Format | 90 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Interfaces, Ports & Protocols Baseline | Contractor Determined Format | 90 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Service Support  Functions and  Integration Plan | Contractor Determined Format | 30 Calendar Days after Contract Award | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Records  Management  Architecture/  Integration Plan | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Cybersecurity  Monitoring Strategy | Contractor Determined Format | 30 Calendar Days after Contract Award | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Transition/  Decommission Plan | Contractor Determined Format | 30 Calendar Days after Contract Award | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Requirements  Management Plan / Traceability Matrix | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | Weekly, as  required |
| Customer  Communication Plan | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| White Papers,  Information Papers and Decision  Papers | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | Monthly, as  required |
| Briefing Slides | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | Weekly, as  required |
| \* **Standard Distribution:**   1. 1 copy of the transmittal letter without the deliverable to the Contracting Officer shall be uploaded to <https://www.ditco.disa.mil/dcop/Public/ASP/dcop.asp>. 2. 1 copy of the transmittal letter with the deliverable to the Primary COR or Government designated repository. | | | | |

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

The contractor shall provide an independently-operable system (i.e. able to operate when disconnected from the main cloud service) that allows for continuity of operations while experiencing a Denied, Disconnected, Intermittent or Limited Bandwidth condition IAW section 6 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.). The contractor shall plan for these variations in D-DIL service based on a per tenancy or stand-alone environments that are implemented.

#### Subtask 1 – NIPRNet Environment

Engineer, configure and deploy a standalone, independently operable suite that operates from the NIPRNet cloud instance when connected. The D-DIL solution shall communicate with the cloud to receive updates. It is understood that in some cases, D-DIL deployments may experience lower cloud service availability rates. However, the contractor shall ensure that standalone equipment is engineered and configured to have the same availability and survivability Service Level Agreement (SLA) as that of the cloud.

#### Subtask 2 – SIPRNet Environment

Engineer, configure and deploy a standalone, independently operable suite that operates from the SIPRNet cloud instance when connected. The D-DIL solution shall communicate with the cloud to receive updates. It is understood that in some cases, D-DIL deployments may experience lower cloud service availability rates. However, the contractor shall ensure that standalone equipment is engineered and configured to have the same availability and survivability SLA as that of the cloud.

**Deliverables**

The Government shall require the following documents as the deliverables for this task and sub-tasks. The contractor shall incorporate these deliverables into the proposed PWS. In addition, 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.

| Deliverable Title | Format | **Due Date** | **Distribution** | **Frequency** |
| --- | --- | --- | --- | --- |
| Implementation Plan | Contractor Determined Format | 30 Calendar Days after Award | Standard  Distribution\* | One Time Update annually as required |
| Work Breakdown Schedule (WBS) | Contractor Determined Format | Monthly, on 5th workday  after TO  Execution | Standard  Distribution\* | Monthly, as  required |
| Integrated Master Schedule (IMS) | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | Monthly, as  required |
| Integration Plan | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Architecture, DoDAF  Artifacts/Diagrams (AV, OV, SV, StdV, CV) | Contractor Determined Format | 90 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Interfaces, Ports & Protocols Baseline | Contractor Determined Format | 90 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Cybersecurity  Monitoring  Strategy | Contractor Determined Format | 30 Calendar Days after Contract Award | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Transition/  Decommission Plan | Contractor Determined Format | 30 Calendar Days after Contract Award | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Requirements  Management Plan / Traceability Matrix | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | Weekly, as  required |
| White Papers,  Information Papers and Decision  Papers | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | Monthly, as  required |
| Briefing Slides | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | Weekly, as  required |
| \* **Standard Distribution:**   1. 1 copy of the transmittal letter ***without the deliverable*** to the Contracting Officer shall be uploaded to <https://www.ditco.disa.mil/dcop/Public/ASP/dcop.asp>. 2. 1 copy of the transmittal letter ***with*** the deliverable to the Primary COR or Government designated repository | | | | |

## Task 4 – User Tenancy Stand-Up

The Government will allow flexibility and expects the contractor to propose a tenancy structure. As a result, the contractor shall propose a single tenancy or multitenancy architecture, which meets the requirements of the FRD, and allows each Combatant Commands, Services and Agencies (CC/S/As) the ability to control their own environment from an administrative and operations perspective, while providing logical groupings of users who share common access, attributes and work relationships.

Tenants should be expected to have control of their own instance, including their data, configuration, as well as user, feature, and functionality management. This includes the ability to grant/remove administrative privileges, user roles, and the ability to control license assignment within the solution.

The following table provides a summary of potential DoD subscribers per region. The contractor tenancy structure must address the concerns listed above, as well as an approach for customers that may be part of a CC/S/As at the same time (i.e. “dual hatting”).

| Region | Population |
| --- | --- |
| United States Territories and Possessions | 2,586,638\* |
| Locations outside of the United States  Territories and Possessions | 290,984\* |
| \*DMDC Active Duty, Reserve, and Civilians data as of September 30, 2017; excludes contractors | |

If offering a multitenant environment, the contractor at a minimum must support the establishment of the following tenants: Army, Navy, Marine Corps, Air Force, Coast Guard, Intel Community (IC) (National Security Agency (NSA), National Geospatial-Intelligence (NGA), Defense Intelligence Agency (DIA)) 4th Estate (Defense Health Agency (DHA), DISA, Defense Logistics Agency (DLA), Joint Service Provider (JSP)), COCOMs (Northern Command (NORTHCOM), Transportation Command (TRANSCOM), Strategic Command (STRATCOM)).

Additional tenants may be required by the Government based on future demand and mission requirements. The contractor shall propose the stand-up costs for the notional summary provided above per tenant, to include establishing the new tenancy, as well as the sustainment costs for supporting a maximum of 20 tenants for the proposed CSO.

**Deliverables:**

The Government shall require the following documents as the deliverables for this task and sub-tasks. The contractor shall incorporate these deliverables into the proposed PWS. In addition, 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.

| Deliverable Title | Format | **Due Date** | **Distribution** | **Frequency** |
| --- | --- | --- | --- | --- |
| Tenancy  Architecture | Contractor Determined Format | 30 Calendar Days after PDR\*\* | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Cloud Service  Administration  Portal Plan | Contractor Determined Format | 30 Calendar Days after PDR\*\* | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Directory  Services  Synchronization Plan | Contractor Determined Format | 30 Calendar Days after PDR\*\* | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Hybrid Deployment Strategy | Contractor Determined Format | 30 Calendar Days after PDR\*\* | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Support model and Service Requests Plan | Contractor Determined Format | 30 Calendar Days after PDR\*\* | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Content Management Migration Strategy | Contractor Determined Format | 30 Calendar Days after PDR\*\* | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Email Migration Strategy | Contractor Determined Format | 30 Calendar Days after PDR\*\* | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Multiple Domain Management  Approach | Contractor Determined Format | 30 Calendar Days after PDR\*\* | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Briefing Slides | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | Weekly, as  required |
| \* **Standard Distribution:**   1. 1 copy of the transmittal letter without the deliverable to the Contracting Officer shall be uploaded to <https://www.ditco.disa.mil/dcop/Public/ASP/dcop.asp>. 2. 1 copy of the transmittal letter with the deliverable to the Primary COR or Government designated repository.   **\*\* Preliminary Design Review (PDR):**   1. Deliverable will not be required until the PDR milestone has been reached as indicated within the Contractors proposed Integrated Master Schedule (IMS). | | | | |

## Task 5 – Subscription Licenses

The contractor shall propose per-seat subscription-based pricing, and corresponding licensing model, which allows the Government to purchase or subscribe to the contractor CSO, a la carte, for a specific period and for a set price. In addition, the contractor shall provide a licensing strategy (i.e. process/procedures, mechanism) describing the contractor approach to license management, process for tracking licenses consumed by tenants, and how subscribers can transition from one user tier to another, to give the government the ability to track who has subscribed to the CSO, and has been granted access to a specific function, service or product.

#### Subtask 1 – Core Services

The contractor shall provide a user tiered subscription based licensing structure that provides services for the functionality outlined in Figure 1. The number of users within each licensing tier will be specified at the task order-level based upon the DoD consumer’s mission requirements. In addition to Figure 1, the following table below provides an example licensing structure that maps different types of users to features and client types. Table 1 is to be used as a ***reference only*** for the licensing structure the Government is requesting. The contractors shall propose a tiered user licensing structure utilizing Attachment 6 based on the current market place offering for the proposed CSO.

Table 1 – Notional Core Service User Tiers

| Type of User | Features Breakdown | **Types of Clients** |
| --- | --- | --- |
| **Economy User** | Messaging capabilities (i.e. email, calendar, contacts) plus records management and legal search and hold. | * 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) | * Standalone/Thick * Mobile * Virtual Desktop * Web Browser |
| **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 productivity suite (i.e. word processor, spreadsheet, and presentation). Other enhanced business applications used by a smaller subset of users (e.g. project scheduling) available on per user request. | * Standalone/Thick * Mobile * 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 * Virtual Desktop * Web Browser |

#### Subtask 2 – Drafting and Diagraming

The contractor shall identify the per user license for Drafting and Diagramming services IAW the FRD requirements PS-020 and PS-021.

#### Subtask 3 – Project Management

The contractor shall identify the per user license for Project Management services, IAW the FRD requirements PS-022, and PS-023.

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

In addition to the tiered user licensing structure identified for sub-task(s) 5.5.1, 5.5.2, and 5.5.3 the contractor shall independently indicate utilizing Attachment 6 any additional service/add-ons/plug-ins user licenses (i.e. Geographic Information Science) that can be utilized/purchased with the proposed CSO.

**Deliverables**

The Government shall require the following documents as the deliverables for this task and sub-tasks. The contractor shall incorporate these deliverables into the proposed PWS. In addition, 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.

| Deliverable Title | Format | **Due Date** | **Distribution** | **Frequency** |
| --- | --- | --- | --- | --- |
| Software License Management Plan | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Software License  Reports | Contractor Determined Format | Monthly, on 5th workday  after TO  Execution | Standard  Distribution\* | Monthly, as  required |
| Licensing &  Subscription  Structure | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Briefing Slides | Contractor Determined Format | 30 Calendar Days after TO Execution | Standard  Distribution\* | Weekly, as  required |
| \* **Standard Distribution:**   1. 1 copy of the transmittal letter without the deliverable to the Contracting Officer shall be uploaded to <https://www.ditco.disa.mil/dcop/Public/ASP/dcop.asp>. 2. 1 copy of the transmittal letter with the deliverable to the Primary COR or Government designated repository. | | | | |

## 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 on a per-tenant basis:

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

The contractor shall interoperate the NIPRNet CSO to the Softswitch (SS) backbone by establishing an Assured Service (AS) Session Initiation Protocol (SIP) trunk from the DEOS edge via a contractor provided AS-SIP Gateway to the Government provided Session Border Controller (SBC). Otherwise, the contractor shall configure a SIP trunk to the Government provided SBC to enable interoperability with DISA’s NIPRNet SS backbone IAW the DEOS FRD section 8.1.3.

#### 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 8.1.4.

#### Subtask 3 – Mass Warning Notification

The contractor shall provide integration or interoperability with Service or Component mass warning notification systems IAW the FRD section 8.6.

#### Subtask 4 – Local Voice Survivability

The contractor shall provide local voice survivability during wide-area networks (WAN) failures that prevent end instruments/clients from registering and signaling to the centralized voice session managers, IAW the FRD section 8.1.6

#### Subtask 5 – E-911

The contractor shall ensure E911 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 8.1.5.

#### 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 8.1.7.

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

The contractor shall interoperate the NIPRNet CSO to the SS backbone by establishing an AS SIP trunk from the DEOS CSO edge via a contractor provided AS-SIP Gateway to the Government provided SBC. Otherwise, the contractor shall configure a SIP trunk to the Government provided SBC to enable interoperability with DISA’s NIPRNet SS backbone. In addition, the contractor shall support E.164 number routing, the DoD’s World-Wide Numbering & Dial Plan, as well as assign Defense Switched Network (DSN) and commercial phone numbers to subscribers/end instruments in accordance with the FRD section 8.1.1.

#### 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) network, which provides Public Switched Telephone Network (PSTN) access to DoD IAW the FRD section 8.1.2.

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

The contractor shall interoperate the NIPRNet CSO to individual Local Session Controllers on a tenant-per-tenant basis, by establishing SIP trunks IAW the DEOS FRD section 8.1.8.

#### Subtask 10 – SS Backbone – Video

The contractor shall interoperate the NIPRNet CSO to the SS backbone to enable video communications IAW the FRD section 8.2.1.

#### Subtask 11 – Unclassified Global Video Service (GVS-U)

The contractor shall interoperate the NIPRNet CSO to unclassified DISA Global Video Service (GVS) using SIP or H.323 trunks IAW the FRD section 8.2.2.

#### Subtask 12 – Classified Global Video Service (GVS-C)

The contractor shall interoperate the SIPRNet CSO to classified DISA GVS using SIP or H.323 trunks IAW the FRD section 8.2.3.

#### Subtask 13 – EVoIP – Video

The contractor shall interoperate the NIPRNet CSO to the SS backbone to enable video communications IAW the FRD section 8.2.4.

#### Subtask 14 – ECVoIP – Video

The contractor shall interoperate the SIPRNet CSO to DISA ECVoIP Session Managers to enable video communications IAW the FRD section 8.2.5.

#### Subtask 15 – Cross Domain Enterprise Services

The contractor shall interface the NIPRNet CSO to existing Cross Domain Services (CDSs) to transfer data between security domains, based on user demand and on a per-tenant basis IAW the FRD section 8.3.1.

#### Subtask 16 – SIPR Cross Domain Enterprise Services

The contractor shall interface the SIPRNet cloud service offering to existing CDSs to transfer data between security domains, based on user demand and on a per-tenant basis IAW the FRD section 8.3.1.

#### Subtask 17 – NIPR Global Content Directory Services (GCDS)

The contractor shall leverage the Global Content Delivery Service (GCDS) to accelerate the delivery of NIPRNet CSO content and applications across the DoDIN IAW the FRD section 8.4.

#### Subtask 18 – 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 8.4.

#### Subtask 19 – 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 8.5.

#### Subtask 20 – 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 8.5.

#### Subtask 21 – Records Management

Provide integration or interoperability with the CSO to support the National Archives and Records Administration (NARA) and comply with [DoDI 5015.02](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/501502p.pdf), and the FRD section 5.

#### Subtask 22 – Workflow

Provide integration or interoperability with the CSO to support declassification review, legal-related reviews, and approval processes IAW the FRD section 5.1.

#### Subtask 23 – Redaction

Provide integration or interoperability with the CSO to support Document Redaction IAW the FRD section 5.2.

#### Subtask 24 – Freedom of Information Act (FOIA)

Provide integration or interoperability with the CSO to support create and preserve records IAW the FRD section 5.3.

#### Subtask 25 – eDiscovery

Provide integration or interoperability with the CSO to support documentation marking, redactions, and deduplication of files IAW the FRD section 5.4.

**Deliverables:**

The Government shall require the following documents as the deliverables for this task and sub-tasks. The contractor shall incorporate these deliverables into the proposed PWS. In addition, 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.

| Deliverable Title | Format | **Due Date** | **Distribution** | **Frequency** |
| --- | --- | --- | --- | --- |
| Integration Plan | Contractor Determined  Format | 30 Calendar Days after CDR\*\* | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Infrastructure  Review Checklist | Contractor Determined  Format | 30 Calendar Days after CDR\*\* | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Infrastructure  Analysis/Evaluation Report | Contractor Determined  Format | 30 Calendar Days after CDR\*\* | Standard  Distribution\* | One Time;  Updated  annually as  required |
| \* **Standard Distribution:**   1. 1 copy of the transmittal letter without the deliverable to the Contracting Officer shall be uploaded to <https://www.ditco.disa.mil/dcop/Public/ASP/dcop.asp>. 2. 1 copy of the transmittal letter with the deliverable to the Primary COR or Government designated repository.   **\*\* Critical Design Review (CDR):**   1. Deliverable will not be required until the CDR milestone has been reached as indicated within the Contractors proposed Integrated Master Schedule (IMS). | | | | |

## Task 7 – Data and Readiness Assessments

The contractor shall perform a comprehensive evaluation of DoD customers legacy infrastructure and data that will be migrated to the DEOS service. Evaluations shall clearly detail traffic flow, system components, applications, and integration dependencies, at a minimum, and shall retain customer profiles and customer data stored on the legacy systems.

#### Subtask 1 – Directory Service

The contractor shall analyze the existing enterprise directory, and other customer directories, identity services, and domains, to identify the necessary execution activities, migration plan, and implementation required to optimize the existing directory environments in support of migrating directory data into the new DEOS service. Examples include directory object normalization, non-person entity 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 DEOS 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. Revocation status shall be determined by looking up the user-provided certificate in a locally stored Certification Revocation List (CRL) or via an Online Certificate Status Protocol (OCSP) call across the network to the Robust Certificate Validation Service (RCVS).

#### Subtask 2 – Email

The contractor shall assess existing email environments and data to ensure an optimum migration. Examples of activities include, but are not limited to the evaluating email profiles, email data volume, PST data volume, POD architecture/locations, identification and cleanup of defunct mailboxes, distribution lists and delegations, and upgrades of legacy hardware (i.e. servers).

#### Subtask 3 – Content Management

The contractor shall analyze existing content management environments and data to ensure an optimum migration. Examples of activities include site structure/content analysis, site content volume, identification and cleanup of folder hierarchies, determining user permissions, and ensuring workflows compliance.

#### Subtask 4 – Instant Messaging (IM), Chat, & Presence

The contractor shall assess existing IM/chat environments and data to ensure an optimum migration. Examples include IM/chat profiles, IM/chat contact lists, persistent chat group migration, analysis of messages stored in persistent chat groups, and on a case by cases basis analysis of chat federation with other systems.

#### Subtask 5 – Productivity Suite

The contractor shallevaluate theproductivity suite environment and data to ensure an optimum migration. Examples include updating thick applications prior to migration, cleaning and reducing duplicate files, and normalizing document versions before starting the migration.

#### Subtask 6 – Web Conferencing

The contractor shall analyze the existing web conferencing environment and data to ensure an optimum migration. Examples include evaluating persistent conferences, access control and delegation of users to persistent web conferences, persistent web conference content volume, analyzing local network configuration, bandwidth availability and overall readiness, and identification and cleanup of folder hierarchies.

#### Subtask 7 – File Storage

The contractor shall assess existing local user data environments to ensure an optimum migration. Examples include analyzing content and volume of files located in local device stores (e.g. desktops, hard drives), as well as network drives.

#### Subtask 8 – Native Audio

The contractor shallevaluate existing native audio environments to ensure optimum migration. Examples include migrating contact lists, call logs, analyzing local network configuration, bandwidth availability and overall readiness for native audio traffic.

#### Subtask 9 – Native Video

The contractor shallevaluate existing native video environments to ensure optimum migration. Examples include migrating contact lists, call logs, analyzing local network configuration, bandwidth availability and overall readiness for native video traffic.

**Deliverables:**

The Government shall require the following documents as the deliverables for this task and sub-tasks. The contractor shall incorporate these deliverables into the proposed PWS. In addition, 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.

| Deliverable Title | Format | **Due Date** | **Distribution** | **Frequency** |
| --- | --- | --- | --- | --- |
| Core Capability Data Readiness Plan | Contractor Determined Format | Draft 45 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Core Capability Data Readiness  Review Checklist | Contractor Determined Format | Draft 45 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  monthly as  required |
| Core Capability Analysis/Evaluation Report | Contractor Determined Format | Draft 45 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  monthly as  required |
| \* **Standard Distribution:**   1. 1 copy of the transmittal letter without the deliverable to the Contracting Officer shall be uploaded to <https://www.ditco.disa.mil/dcop/Public/ASP/dcop.asp>. 2. 1 copy of the transmittal letter with the deliverable to the Primary COR or Government designated repository. | | | | |

## Task 8 – User & Data Migration

The Government must minimize the business impacts of data migration downtime, data integrity issues, costs, and control problems. The Service Provider will be required to develop a data migration process model and utilize robust methodology (i.e. data profiling) and tools for migrations. The contractor will provide the manpower, tools, and hardware needed to migrate existing services (e.g. DEPS, DEE), as well as the customer data and support operations necessary to deliver the CSO to approximately 3.12 million DoD subscribers. During migration, the contractor shall support dual operations, ensuring that users migrated to the cloud offering are able to collaborate with those that have not been migrated to the cloud. The contractor shall ensure that customer profiles and data stored on the legacy systems are completely 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 establish a link to Identity Synchronization Services (IdSS) via Security Assertion Markup Language (SAML) interface to 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 for provision/de-provisioning of user accounts. The contractor shall provide government authentication using SAML 2.0 integration with a Government specified identity provider utilizing DoD approved multi-factor authentication mechanisms or username and password according to agency policy. 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 mailboxes (e.g. conference rooms), group mailboxes, calendars, contact lists and distribution lists from their legacy systems. The contractor shall also migrate journaled messages as well as files needed for legal or regulatory compliance. The contractor shall ensure coexistence of the legacy email systems with the proposed CSO. The contractor shall migrate mailbox data from production source system to include message store, calendar, and contacts. The contractor shall provide integration between the CSO and Government mobile devices. The contractor shall establish dual delivery of messages during the transition period. After migration, the service shall provide access to historical data that is subject to records management provisions, as well as access to legacy email server archives.

#### Subtask 3 – Content Management

The contractor shallmigrate content management sites, to include structure, content, workflows, and permissions from their 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. The contractor shall provide integration between the cloud content management offering and Government mobile devices. After migration the service shall provide access to historical data that is subject to records management provisions, as well as access to legacy content management archives.

#### Subtask 4 – Instant Messaging (IM), Chat, & Presence

The contractor shall enable IM/Chat & Presence capabilities for all users’ part of the CSO, regardless of tenancy association if using a multitenancy environment. In addition, the contractor shall migrate IM/chat profiles, IM/chat contact lists, persistent chat groups, and messages stored in persistent chat groups from the legacy IM/chat systems to the cloud IM/chat offering. The contractor shall ensure that chat federation with other systems is maintained with the legacy IM/chat system and the CSO IM/chat offering during migration.

#### Subtask 5 – Productivity Suite

The contractor shall migrate legacy word processing, spreadsheet, presentation, database management, and diagramming and project management files from on premise repositories to the CSO. The contractor shall ensure legacy files can be opened and seen in the CSO. During migration, the contractor shall ensure users that have not been migrated can access files/data stores that have been migrated to the CSO.

#### Subtask 6 – Web Conferencing

The contractor shall migrate persistent web conference and prerecorded conferencing sessions from the legacy web conferencing system to the cloud web conferencing offering. The contractor shall ensure access control and delegation of users to persistent web conferences is maintained once migrated. During migration, the Contractor shall ensure users that have not been migrated can access persistent web conferences that have been migrated to the CSO.

#### Subtask 7 – File Storage

The contractor shall migrate individual user data stored in local user data environments (e.g. desktops, hard drives) as well as network drives, into each user’s file storage partition in the cloud offering. The contractor shall ensure access control is maintained once migrated to the cloud offering. During migration, the contractor shall ensure users can access files that have been migrated to the CSO.

#### Subtask 8 – Native Audio

The contractor shall enable native audio calling capabilities for all users’ part of the CSO, regardless of tenancy association if using a multitenancy environment. In addition, the contractor shall migrate legacy DSN and PSTN telephone numbers in E.164 format to subscriber profiles, as well as any voicemail messages required for legal compliance.

#### Subtask 9 – Native Video

The contractor shall enable native video calling capabilities for all users’ part of the CSO, regardless of tenancy association if using a multitenancy environment. In addition, the contractor shall migrate legacy DSN and PSTN telephone numbers in E.164 format to DEOS subscriber profiles, move personal video teleconferences (VTCs) to native video conferences.

**Deliverables:**

The Government shall require the following documents as the deliverables for this task and sub-tasks. The Contractor shall incorporate these deliverables into the proposed PWS. In addition, 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.

| Deliverable Title | Format | **Due Date** | **Distribution** | **Frequency** |
| --- | --- | --- | --- | --- |
| Data Migration & Management Plan | Contractor Determined Format | 45 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Monthly User  Migration Reports | Contractor Determined Format | Monthly, on 5th workday  after TO  Execution | Standard  Distribution\* | Monthly, as  required |
| Migration Strategy | Contractor Determined Format | 45 Calendar Days after TO Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Migration Schedule | Contractor Determined Format | Monthly, on 5th workday  after TO  Execution | Standard  Distribution\* | Monthly, as  required |
| \* **Standard Distribution:**   1. 1 copy of the transmittal letter without the deliverable to the Contracting Officer shall be uploaded to <https://www.ditco.disa.mil/dcop/Public/ASP/dcop.asp>. 2. 1 copy of the transmittal letter with the deliverable to the Primary COR or Government designated repository. | | | | |

## Task 9 – Training

Conduct technical reviews and develop appropriate materials to train system users and instructors in preparation of operational deployments. Assess training requirements based on system and functional baseline. Develop training artifacts in support of operations including but not limited to Standard Operating Procedures (SOPs), and Tactics, Techniques and Procedures (TTPs). Provide online documentation to train users and administrators on the service being provided to include access, troubleshooting guides, features, (i.e. NetOPS) provisions, and capabilities. Documentation and support shall include user groups such as but not limited to Senior Executive Service (SES), Government administrators, and types of end users that will be impacted by consuming the new service

#### Subtask 1 – Classroom/Instructor Led

Provide in-person, classroom/instructor led training to government designated personnel to explain software features, functions, and common tasks associated with DEOS services and capabilities.

#### Subtask 2 – Individual Hands-On

Provide individual hands-on training to Government designated personnel to explain software features, functions, and common tasks associated with DEOS services and capabilities.

#### Subtask 3 – Seminar Style Group Demonstration

Provide live demonstration training in a large group setting to Government designated personnel to explain software features, functions, and common tasks associated with DEOS services and capabilities.

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

Provide the Government with training materials in forms (e.g. Recorded Webinar, Factsheets, etc.) that can be distributed and published to a web portal that will be established and maintained by the Government. The developed materials shall allow users to be able to troubleshoot or perform common tasks, and minor configuration tests on the service.

**Deliverables:**

The Government shall require the following documents as the deliverables for this task and sub-tasks. The Contractor shall incorporate these deliverables into the proposed PWS. In addition, 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.

| Deliverable Title | Format | **Due Date** | **Distribution** | **Frequency** |
| --- | --- | --- | --- | --- |
| Training  Strategy/Plan | Contractor Determined Format | Draft 45 Calendar Days after TO  Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| End User Fact Sheets/Manuals | Contractor Determined Format | Monthly, on 5th workday after TO  Execution | Standard  Distribution\* | Monthly, as  requested |
| System  Administrator Configuration Guides for NIPR, SIPR, and D-DIL  Environments | Contractor Determined Format | Monthly, on 5th workday after TO  Execution | Standard  Distribution\* | Monthly, as  requested |
| Training  Requirements  Definition | Contractor Determined Format | Draft 45 Calendar Days after TO  Execution | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Training  Material | Contractor Determined Format | Monthly, on 5th workday after TO  Execution | Standard  Distribution\* | Monthly, as  required |
| Training  Feedback Forms | Contractor Determined Format | Monthly, on 5th workday after TO  Execution | Standard  Distribution\* | Monthly, as  required |
| \* **Standard Distribution:**   1. 1 copy of the transmittal letter without the deliverable to the Contracting Officer shall be uploaded to <https://www.ditco.disa.mil/dcop/Public/ASP/dcop.asp>. 2. 1 copy of the transmittal letter with the deliverable to the Primary COR or Government designated repository. | | | | |

## Task 10 – Engineering Support

This section outlines requirements for technical/engineering support services with expertise in both traditional IT infrastructure and cloud computing. Support services may be provided to the DEOS Program Management Office (PMO) directly, or to DEOS consumers. Provide the full range of engineering support necessary to incorporate new/future technologies into the DEOS Service/Baseline subsequent to initial deployment.

### Subtask 1 – General Engineering Support

The contractor shall assist with the technical, detailed, management of initiatives and to assist in the design, implementation, modification, sustainment, and portfolio management of DEOS programs, projects, and work activities for currently ongoing issues, or new issues as they arise. The scope includes comprehensive technical/engineering support services to active projects, programs, and work activities, as well as any future work efforts as they arise or are identified for both NIPRNet and SIPRNet activities.

The contractor shall provide the DEOS PMO and DoD consumers with experienced personnel who are knowledgeable in cloud computing, engineering, infrastructure development and design, native audio, native video, content management development, records management, collaboration services, and productivity suites that span United States territories and possessions and Non-United States territories and possessions footprints.

## Task 12 – 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. Provide a Monthly Service Utilization, Capacity, Outage and Upgrade Status and Forecast Report and resources (i.e. personnel) required for close-out operations prior to contract completion.

**Deliverables:**

The following deliverables represent the standard deliverables that the Government will require for this task order and any sub-tasks. The contractor shall incorporate these deliverables into the proposed PWS. In addition, 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Deliverable Title | Format | **Due Date** | **Distribution** | **Frequency** |
| Task Order  Management Plan | Contractor Determined Format | 30 Calendar Days after Award | Standard  Distribution\* | One Time;  Updated  annually as  required |
| Monthly Budget  Report | Contractor Determined Format | Monthly, on 5th workday after TO Execution | Standard  Distribution\* | Monthly, as  required |
| Monthly Service Utilization, Capacity, Outage and Upgrade Status and Forecast Report | Contractor Determined Format | Monthly, on 5th workday after TO Execution | Standard  Distribution\* | Monthly, as  required |
| Work Breakdown Structure (WBS) | Contractor Determined Format | Monthly, on 5th workday after TO Execution | Standard  Distribution\* | Monthly, or as requested |
| \* **Standard Distribution:**   1. 1 copy of the transmittal letter without the deliverable to the Contracting Officer shall be uploaded to <https://www.ditco.disa.mil/dcop/Public/ASP/dcop.asp>. 2. 1 copy of the transmittal letter with the deliverable to the Primary COR or Government designated repository. | | | | |

# Performance Standards

Performance Standards define the level of service required under the contract and subsequent task orders to successfully meet the performance objectives. The performance standards specified in the table below represent the baseline for the Acceptable Quality Levels (AQLs) for task orders issued under the DEOS contract. The RFP Test & Evaluation addendum provides additional functional and performance metrics the contractor shall meet. At a minimum, all the AQLs listed in the Table 3 shall be included and addressed within the PWS. Based upon their proposed technical and management solution, the contractor 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. The contractor shall also propose a separate Quality Assurance Surveillance Plan (QASP) using the required QASP format provided as Attachment 5 to the solicitation. The QASP shall address the specific methodologies that the Government shall utilize to surveil performance under the task orders.

Table 2 – Government Defined AQLs

|  |  |  |  |
| --- | --- | --- | --- |
| Performance Standard | Reference | AQL or Tolerance | Method of  Surveillance |
| Availability | FRD –  System Wide | Provide 99.9% availability of services.  NOTE: The 99.9% availability is limited to the service provided by the CSP, not the underlying transport, or delivery to the end user. | * Random Sampling * Trend Analysis |
| Capacity | N/A | For solutions hosted in DoD datacenters, ensure that the ratio of the workload to the capacity of the available infrastructure does not exceed 95%. The ratio is calculated by tracking average utilization over time of workloads with varying demand, and working from the mean to find the capacity to handle 95% of all workloads. The Government will perform capacity planning at least once a month. The capacity planning shall verify that the local load balancing/sharing is adequate or if additional servers or other associated equipment are needed. | * Trend Analysis |
| Elasticity | N/A | For solutions hosted in DoD datacenters, support elasticity for up to 80% of the computing and traffic load generated by the simultaneous use of DEOS services without failure due to resource exhaustion for each system (e.g., NIPR/SIPR). | * Random Sampling * Trend Analysis |
| Information Security | FRD – Incident Management | Notify the DEOS PMO and other Government designated personnel within 60 minutes of detecting a data breach or data loss in the NIPR environment, and within 30 minutes of detecting a data breach or data loss in the SIPR environment. | * Trend Analysis * Third-party Audits |
| Access  Management | FRD – Access Management | Provision accounts within 30 minutes of the CSP receiving a single subscriber account request. | * Trend Analysis * Customer Feedback |
| Business  Continuity | FRD –  System Wide | Provide a Recovery Point Objective (RPO) of < 45 minutes per event. | * Trend Analysis * Third-party Audits |
| Disaster  Recovery | FRD –  System Wide | Provide a Recovery Time Objective (RTO) of <2 hours per event. | * Trend Analysis * Third-party Audits |
| Encryption | FRD –  System-Wide | Encrypt data in transit and at rest to comply with DoD specifications, except for points where Break & Inspect (B&I) is necessary. | * Random Sampling |
| Service Desk  Response | FRD –  Service Desk | Respond within 15 minutes for catastrophic incidents; within 1 hour for critical incidents; within 4 hours for major incidents; and within 2 business days for normal incidents | * Trend Analysis * Customer Feedback |
| D-DIL  Reconnection | FRD -  D-DIL | Support quick authentication and reconnect (< 30 seconds). | * Trend Analysis * Customer Feedback |
| Event  Management | FRD – Event Management | Collect system performance data every N seconds on a continuous basis. The value N must be configurable, and have a default value of 300. | * Trend Analysis |
| Incident  Management | FRD – Incident Management | Notify the DEOS PMO and other Government designated personnel within 60 minutes of detecting an outage | * Trend Analysis * Third-party Audits |
| Intellectual Property / Data Loss | FRD – System-Wide | Report an intellectual property or Data Loss violation within 4 hours of detection to the Government. | * Trend Analysis * Third-party Audits |
| Incident  Management | FRD – Incident Management | Provide root-cause reports and fixes for major outage occurrence resulting in greater than 1-hour of unscheduled downtime. | * Periodic Sampling |
| Service Desk | FRD – Service Desk | Provide Live Agent Tier 3 support during normal business hours, allowing customer service desk interactions for submitting incidents using telephone and email, at a minimum. | * Random Sampling * Customer Feedback |
| Service Desk | FRD – Service Desk | Provide the ability to submit service requests 24 hours per day, 7 days per week, with Tier 3 on call support after hours as situations arise that require advanced engineering. | * Random Sampling * Customer Feedback |
| Email  Retention | FRD - Email | Retain deleted items for a configurable duration, with a default of 30 days. | * Random Sampling |

## Method of Surveillance Definitions

The Government has defined the following methods of Surveillance for the AQLs or Tolerances outlined in Table 1 of section 6.

#### Random Sampling

Random sampling is a statistically based method that assumes receipt of acceptable performance if a given percentage or number of scheduled assessments is found to be acceptable. The results of these assessments help determine the government's next course of action when assessing further performance of the contractor. If performance is considered marginal or unsatisfactory, the evaluators should document the discrepancy, begin corrective action and ask the contractor why their quality control program failed. If performance is satisfactory or exceptional, they should consider adjusting the sample size or sampling frequency. Random sampling is the most appropriate method for frequently recurring tasks. It works best when the number of instances is very large and a statistically valid sample can be obtained. The Government will be responsible for executing Random Sampling events and capturing data, but may from time to time request assistance from the contractor to execute these activities.

#### Periodic Sampling

Periodic sampling is similar to random sampling, but it is planned at specific intervals or dates. It may be appropriate for tasks that occur infrequently. Selecting this tool to determine a contractor's compliance with contract requirements can be quite effective, and it allows for assessing confidence in the contractor without consuming a significant amount of time. The contractor will be responsible for executing Periodic Sampling events, capturing data and generating reports on behalf of the Government.

#### Trend Analysis

Trend analysis should be used regularly and continually to assess the contractor's ongoing performance over time. It is a good idea to build a database from data that have been gathered through performance assessment. Additionally, contractor-managed metrics may provide any added information needed for the analysis. This database should be created and maintained by government personnel. The contractor will be responsible for executing Trend Analysis events, capturing data and generating reports on behalf of the Government.

#### Customer Feedback

Customer feedback is firsthand information from the actual users of the service. It should be used to supplement other forms of evaluation and assessment, and it is especially useful for those areas that do not lend themselves to the typical forms of assessment. However, customer feedback information should be used prudently. Sometimes customer feedback is complaint-oriented, likely to be subjective in nature, and may not always relate to actual requirements of the contract. Such information requires thorough validation. The Government will be responsible for capturing customer feedback, but may request assistance from the contractor on a case by case basis.

#### Third-party Audits

The term "third-party audit" refers to contractor evaluation by a third-party organization that is independent of the government and the contractor. All documentation supplied to, and produced by, the third party should be made available to both the Government and the contractor. Remember, the QASP should also describe how performance information is to be captured and documented. This will later serve as past performance information. Effective use of the QASP, in conjunction with the contractor's quality control plan, will allow the Government to evaluate the contractor's success in meeting the specified contract requirements. Those assessment methods identified in the QASP, together with the contractor's quality control plan will help evaluate the success with which the contractor delivers the level of performance agreed to in the contract. The Government will hire independent third-party entities to evaluate the contractor, nonetheless the contractor shall comply with the third-party requests for information relating to the audits.

# Incentives

The identification of incentives (both positive and negative) will be addressed in each task order and reported in Contractor Performance Assessment Reporting System (CPARS). Each requirement will address both positive and negative incentives where practical. 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. Additional incentives and disincentives may be defined in subsequent task orders.

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. Failure to meet the AQLs specified in Section 7 or to submit deliverables in a relevant and timely manner may result in an unsatisfactory past performance report by the Government. Additionally, the Government will determine the level of performance as a factor in the determination to exercise additional options for continuity of services or addition of capacity or capabilities.

## Operational Availability Performance Standards

In addition, failure to meet the Performance Standards tabulated in Section 6 of the SOO and the various metrics outlined through Attachment 2, (FRD). The contractor may also result in an unsatisfactory CPAR rating by the Government. Additionally, the Government will use adequacy of performance as a factor in determining whether to exercise additional options for continuity of services, additional capacity or capabilities. The following service interruptions will not be counted against the contractor for:

* Interruptions caused by the negligence of the Government or others authorized by the Government to use the Government's service.
* Interruptions due to the failure of power, equipment, systems or connections not provided by Contractor or sub-contractors.
* Interruptions during any period when the Government has released the service environment for maintenance or rearrangement purposes or for the implementation of a Government order.
* Interruptions that continue because of the Government's failure to authorize replacement of any element of special construction. The period for which credit is not allowed begins on the 7th day after the Government receives the contractor’s written notification of the need for such replacement. It ends on the day after receipt of the Government's written authorization for such replacement.
* Interruptions during periods when the Government elects not to release the private service environment for testing and/or repair.

Service Level Agreements

* Minimum Service Level accepted will be 99.9% Operational Availability Rate calculated monthly.
* All proposals will provide the cloud provider service level agreement to include incentives and exclusions for evaluation.

# Place of Performance

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 (e.g. corporate, 3rd party, or subcontractor). The Government will, if required, further specify the Periodic Progress Meetings at the task order level.

The contractor shall specify all service locations by facility name, point of contact, description, geographic location and address. DISA requires at least two full time equivalent security specialists certified as Information Assurance Officers to be available for periodic meetings and support at the DISA Headquarters Facility at Fort Meade, MD location. However, it is not the intent of the Government that these or any other representatives shall have office locations at Government offices or sites that may be specified and/or required at task order level.

Travel in and around the primary place of performance may be required throughout the period of performance. Additional travel within may be required to support the requirements of this contract.

## 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. Contractor shall prepare all deliverables and other contract documentation utilizing contractor resources. 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 (KO) 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 ID/IQ contract will be a 5-year base period with five 1-year option period and the 6-month extension of services IAW FAR 52.217-8. 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

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.

## References

1. DISA Form 786, DISA Statement of Information System Use and Acknowledgement of User Responsibilities
2. DISA Policy Letter, Unauthorized Connections to Network Devices, 11 September 2013
3. DISAI 240-110-8, Information Security
4. DISAI 240-110-36, Personnel Security
5. DISAI 240-110-38, Industrial Security
6. DISA Instruction 630-230-19, Cybersecurity
7. DoDM 5200.01, Vol 1-4 Information Security Program, 24 February 2012
8. DOD 5200.2-R, DoD Personnel Security Program
9. DOD 5220.22-M, National Industrial Security Program Operating Manual, February 2006 Incorporating Change 02 May 2016
10. DOD 5220.22-R, Industrial Security Regulation
11. DoDM 5105.21 Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security (if applicable)

# Facility Security Clearance

The work to be performed under this Contract may be executed up to the Top Secret level and may require Sensitive Compartmented Information (SCI) access eligibility for some personnel. Other than small businesses must have, at a minimum, final Secret Facility Clearance (FCL) from the Defense Security Service (DSS) Facility Clearance Branch (FCB) at time proposals are due. Small businesses are not required to have a clearance at the time proposals are due. However, they must have the FCL before they are eligible to compete on Task Orders requiring FCLs.

## Facility Safeguarding

The work performed, and information residing at the contractor’s facility will be up to the Secret and NATO Secret level, and must be protected as such. Therefore the company must have a Secret Level of Safeguarding in place.

## Facility Escorts

In cases where a non-cleared subject matter expert is needed to troubleshoot technical issues, a properly background checked individual will conduct an escort session for this work. During the escort session the security escort would ensure that the non-qualified (i.e. lacking the required background screening for un-escorted access) escortee did not have access to customer data or ability to detrimentally impact the availability or integrity of the system.

**In the below description:**

1. “Non-qualified” means specifically any staff who have not completed the necessary background screening standard in order to have un-escorted access.
2. “Sensitive customer data” includes the following data types in the Cloud Hosted Enterprise Services:
   * **Customer Content:** Emails, documents, structured and storage data containing customer proprietary information.
   * **End User Identifiable Information:** Information about users of the system which is protected under the Privacy Act of 1974.

**All escort sessions must be conducted in accordance with the following standards:**

1. Security escort is conducted by an individual who has passed the background screening standard required for the required level of access to the environment.
2. Security escort is conducted by an individual with sufficient background knowledge of the system to monitor the activities of the non-qualified escortee.
3. Security escort is accountable to ensure that the actions of the non-qualified escortee do not result in exposure of sensitive customer data, or impact to the integrity and availability of the system.
4. If the security escort detects any action by the non-qualified escortee that results in exposure of sensitive customer data, destruction or alteration of sensitive customer data, or impact to the system integrity or availability – whether intentional, unintentional, or even potential, this must be escalated to the appropriate team as a potential security incident for investigation and determination.

**All escort sessions must log the following information:**

* Person escorted
* Person escorting
* Reason for escort
* Time and duration of the escort

1. Any software or hardware brought into a secure environment must be screened for malicious code before ingress or for unauthorized content on egress.
2. Security escort is accountable to ensure any ability of the non-qualified escortee to access the system is removed at the end of the escort session.
3. Security escort must not leave the non-qualified escortee unattended at any time during the escort session.
4. Security escort must ensure that the actions taken during the escort session do not modify the system in any way that would allow non-qualified staff access to systems or data that require background screening per the offering’s current standard.

### Physical Escort Standards

Technical Subject Matter Experts and 3rd party vendor representatives who, as un-qualified escorted, are escorted into the physical security boundary may have hands-on access to system infrastructure, as long as this occurs under the supervision of the security escort.

This section shall be considered a supplement to block 13 of the Government provided DD Form 254, Contract Classification Specification. In addition, the contractor shall provide a work breakdown structure for positions requiring government clearances and background investigations (IT-I, IT-II) for government approval, listing will include number and brief description of duties.

# Security Clearance and Information Technology (IT) Level

All personnel performing on this contract will be U.S. citizens. There are two IT Level Classifications, IT-I and IT-II. Personnel security requirements will be determined at the task order level.

## Personnel Clearances

All personnel requiring SCI, Top Secret or IT-I access under this contract/order shall undergo a favorably adjudicated Tier 5 (T5) investigation (formerly known as a Single Scope Background Investigation (SSBI)) as a minimum requirement. The T5 will be maintained current within 5-years and requests for T5 reinvestigation or Phased Periodic Reinvestigation (PPR) will be initiated prior to the 5-year anniversary date of the previous Tier 5.

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 T3 investigation request prior to the 10-year anniversary date of the previous T3 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/order 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, Single Scope Background Reinvestigation, or PPR by any of the DoD Central Adjudication Facility or other federal adjudications facilities within a 5-year period will be automatically accepted for final Secret IT-I access.

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).

## Computing Environment (CE) Certification

Cybersecurity workforce certification is aimed at unifying the overall cyberspace workforce and establishes specific workforce elements (cyberspace effects, cybersecurity, and cyberspace IT to align, manage and standardize cyberspace work roles, baseline qualifications, and training requirements IAW DoD 8140, Cyberspace Workforce Management and DoD 8570.01-M Information Assurance Workforce Improvement Program. The contractor personnel performing cybersecurity workforce functions with privileged-level access to control, manage, or configure Government information systems shall meet training and certification requirements for the level of performance outlined in duty categories for Cybersecurity Support Personnel as specified Department of Defense (DoD) 8570.01-M.

As required by DoD 8570.01-M, paragraph C2.3.9, all contractor personnel supporting cybersecurity functions referenced in DoDI 8570.01-M, Tables C3.T2., C3.T5, C3.T7, C4.T3, C4.T5, C4.T7, C10.T3, C10.T5, and C10.T6 must obtain the appropriate DoD-approved IAT/IAM/IASAE (Level I, II, or III), Cybersecurity baseline certifications. Per DoD 8570.01-M, paragraph C1.4.4.4, DoDI 8570.01-M, Cybersecurity functions apply to all positions with IA (cybersecurity) duties, whether performed as primary or additional/embedded duties.

Contractors will obtain all required cybersecurity certificates prior to contract award. Evidence of current certifications must also be provided to the Government at time of award prior to being engaged with privileged level activities. Evidence should to include with their proposal the type of DoD baseline cybersecurity certification, certification number, certification expiration dates, and the name of the certification provider. All cybersecurity category personnel, whether they perform cybersecurity functions as primary or additional/embedded duty, must be certified based on the cybersecurity functions of the position and remain current on their certifications in order to continue to have authorized unsupervised privileged access to Government networks.

Personnel who are not properly qualified and certified IAW DoD 8570.01-M or who fail to maintain their certification status shall not be permitted privileged access to the DoD networks.

The Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.239-7001 (Information Assurance Contractor Training and Certification) applies to this requirement and is subject to the mandates of DoD 8570.01-M which establishes baseline technical and management IA skills for personnel performing cybersecurity functions within DoD. Functions spanning multiple levels require certification of the highest level functions. Contractor personnel performing functions in multiple categories or specialties shall hold certifications appropriate to the functions performed in each category or specialty. Information Assurance workforce members shall have the certifications corresponding to their IA functions, as defined in Chapters 3, 4, 5, 10, and 11, and Appendix 3 of DoD 8570.01-M at work performance start date. IAT Level I baseline certification is the minimum requirement for unsupervised privileged access. Certification holders shall ensure that their certificates remain active and are renewed prior to expiration. Contractor personnel supporting cybersecurity functions in Chapters 3, 4, 10, and 11 shall be appropriately certified prior to starting work on this contract. The Contractor IA Certification holders shall release their certification information to the DoD through the Defense Workforce Certification Application, https://www.dmdc.osd.mil/appj/dwc/index.jsp.

The contractor shall comply with:

Contracted support personnel assigned to perform cyberspace work roles must meet qualification standards established in supporting issuances, in addition to other existing workforce qualification and training requirements assigned to billets and position requirements in accordance with subpart 239.71 of the DFARS for contracted support designated to perform cyberspace workforce work roles.

If, subsequent to the date of this requirement, the cybersecurity workforce classifications or cybersecurity requirements under this requirement are changed by the Government and if the changes cause an increase or decrease in cybersecurity costs or otherwise affect any other term or condition of this requirement, the requirement shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this requirement.

Contract requirements for maintenance and certification arising from employee turn-overs, etc. will be at the expense of the contractor. The contractor shall not be exempt from meeting any of the contract requirements due to lack of obtaining proper cybersecurity certification requirements.

## 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 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:**  Peggy Durham,Business  Development Center  Acquisition Building  6910 Cooper Ave.  Fort Meade, MD 20755-7088 | **Comm:** (301) 255-8675  **Fax:** (301) 225-0508  **Email:**  disa.meade.bd.mbx.bd-security-managers@mail.mil |

# Information Security and Other Miscellaneous Requirements

## Entry/Exit Security Controls

Contractor personnel must 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 fill positions requiring access to classified information on a DISA contract/order.

## Divulging Classified or Unclassified

The contractor shall not divulge any classified or unclassified information with respect to 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 when a contractor is communicating with the Government or within a Government facility.

## 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 associated contracts, clearly conflict with the interest of the Government.

## For Official Use Only (FOUO) 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.

## Access to Government Facilities, Installations, Operations, Documentation, Databases and Personnel

The contractor shall afford the Government access to the contractor’s facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of data to the function of information technology systems operated on behalf of DISA or DoD, and to preserve evidence of computer crime.

## Government Furnished Property (GFP)/Government-Furnished Equipment

When the task order requires the contractor to work in a Government facility, the Government will furnish or make available working space, network access, and equipment to include, but not limited to:

* Computer
* Telephone (local/long distance calls authorized as dictated by task order performance requirements)
* Facsimile
* Copier
* Printer

The contractor shall comply with the property management processes of the tenant that issues the equipment and will be required to comply with DoD regulations and policies while in utilizing Government Furnished Equipment (GFE).

## Contractor Furnished Equipment (CFE)

Contractor Furnished Equipment (CFE) employed for remote access to a Government network must meet or exceed equivalent GFE cyber security computing requirements. The contractor shall ensure that all CFE (hardware and software) employed to access these environments meet the following minimum Government cyber security requirements and provide periodic certification of compliance as a pre-requisite to being granted network access.

* Use of personally owned systems is prohibited;
* Operating systems and applications must be configured for compliance with the applicable Security Technical Implementation Guides (STIGs);
* DoD approved anti-virus and anti-spyware software must be installed and signatures must be configured to automatically update on a daily basis;
* DoD approved host-level firewall must be utilized and configured to permit traffic by exception only, dropping all other traffic. If the host-level firewall provides intrusion detection or prevention, the signatures or rules must be updated at the same intervals as the anti-virus software;
* Computers must be Information Assurance Vulnerability Management (IAVM) compliant;
* Computers must be scanned with the currently approved DoD scanner solution at a minimum of every 30 days. All vulnerabilities must be remediated and reported to the cognizant Information Assurance Manager;
* Contractor employees must possess a current Government issued CAC and install Government certified CAC readers; and
* Verification of compliance with these requirements must be provided to an appointed Government representative on a monthly basis.

# Other Pertinent Information or Special Considerations

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

## Identification of Potential Conflicts of Interest (COI)

The contactor 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:

1. 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
2. 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
3. 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 OCO 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.

## Facility Inspections

Contractor facilities hosting DoD data shall meet certain Federal Information Security Management Act (FISMA) and DoD security standards as detailed in National Institute of Standards and Technology (NIST) SP 800-53 Revision 4 or later, CNSSI 1253 (27 Mar 14 or later), DoD instructions and the DoD CC SRG.

Routine inspections ensure that facilities are in compliance with these standards. Usually these inspections are conducted by DISA and DISA contractor representatives; however, DISA will review the contractor’s request and plan, subject to DISA approval, for allowing a third party to conduct or support such inspections based on the government’s criteria and process controls.

## Property Accountability

Property accountability requirements will be determined at the task order level. If applicable, the contractor shall submit the attached Electronic Product List (EPL) (see below) in addition to complying with all requirements of DFARS 252.211-7003. See DARS 252.211-9000, Requirement to Submit an Electronic Product List for additional information.



## Data Storage, Rights, and Ownership

In order to implement the provisions at DFARS 252.227-7013(b) and (e), DFARS 252.227-7014(b) and (e), and DFARS 252.227-7017, the contractor shall disclose to the ordering KO and ordering office in any proposal for a task order, or after award of a task order if not previously disclosed in the proposal, any technical data or non-commercial computer software and computer software/source code documentation developed exclusively at government expense in performance of the task order. This disclosure shall be made whether or not an express requirement for the disclosure is included or not included in the solicitation for the order. The disclosure shall indicate the rights asserted in the technical data and non-commercial computer software by the contractor and rights that would be acquired by the government if the data or non-commercial software was required to be delivered under the task order and its contract data requirements list (CDRL) requirements and any cost/price associated with delivery. This disclosure requirement also applies to segregable routines of non-commercial software that may be developed exclusively at Government expense to integrate commercial software components or applications provided under a commercial software license or developed to enable commercial software to meet requirements of the task order. This disclosure obligation shall apply to technical data and non-commercial computer software developed exclusively at Government expense by subcontractors under any task order. Performance of this disclosure requirement shall be considered a material performance requirement of any task order under which such technical data or non-commercial computer software is developed exclusively at Government expense.

## Data Management

The contractor shall establish, maintain, and administer an integrated data management system for collection, control, publishing, and delivery of all program documents. The data management system shall include the following types of documents: CDRLs, White Papers, Status Reports, Audit Reports, Agendas, Presentation Materials, Minutes, Contract Letters, and Task Order Proposals. The contractor shall provide the Government with electronic access to this data, including access to printable reports.

All data, including but not limited to documents, administrative data, support data, and billing data, transmitted via the system or maintained in the system shall reside at all times in servers located in the United States or in servers of which the operation and maintenance are subject only to the laws of the United States. The system will be used to store and transmit sensitive Government and private entity data. Data transmitted must only be subject to disclosure pursuant to U.S. Federal law and not the laws of any other jurisdiction or foreign nation. The contractor has no rights to the DoD’s information/data. For more information on data storage, data rights, and data ownership requirements refer to Section 5.2, Legal Considerations, in the DoD CC SRG.

## Records, Files, and Documents

All physical records, files, documents, and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this SOO, maintained by the contractor which are to be transferred or released to the Government or successor contractor, shall become and remain Government property and shall be maintained and disposed of the Federal Acquisition Regulation (FAR), and/or the DFARS, as applicable. Nothing in this section alters the rights of the Government or the contractor with respect to patents, data rights, copyrights, or any other intellectual property or proprietary information as set forth in any other part of this SOO or the services contract of which this SOO is a part (including all clauses that are or shall be included or incorporated by reference into that contract). The KO may at any time issue a hold notification in writing to the contractor. At such time, the contractor may not dispose of any Government data or Government-related data described in the hold notification until such time as the contractor is notified in writing by the KO, and shall preserve all such data IAW Agency instructions. The contractor shall provide the KO within ten (10) business days of receipt of any requests from a third party for Government-related data. When the Government is using a contractor’s software, the contractor shall provide the Agency with access and the ability to search, retrieve, and produce Government data in a standard commercial format.

## Additional Terms and Requirements

|  |  |  |
| --- | --- | --- |
| Physical Access | 1.01 | (1) The Contractor shall record all physical access to the cloud storage facilities and all logical access to the government data as specified in the Schedule. This shall include the entrant’s name, role, purpose, account identification, entry and exit time. Such records shall be provided to the Contracting Officer or designee in accordance with the Schedule or upon request to comply with federal authorities. |
| Physical Access | 1.02 | (2) As specified by the Contracting Officer, the Contractor shall provide immediate access to all Government data and Government-related data impacting Government data for review, scan, or conduct of a forensic evaluation and physical access to any contractor facility with Government data. If the Government data is co-located with non-Government data, the Contractor shall isolate the Government data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized Government personnel identified by the Contracting Officer, and without the Contractor’s involvement. |
| Personnel Access | 2.01 | The Contactor and any subcontractor personnel shall require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Government in compliance with HSPD -12. At a minimum, all Contractor employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a NACI investigation and be a US person as defined in Executive Order 12333. |
|  |  |  |
| Asset Availability | 4.01 | (1) The Contractor shall inform the Government Contracting Officer’s Representative (COR) of any interruption in the availability of the cloud service as required by the service level agreement. |

|  |  |  |
| --- | --- | --- |
| Asset Availability | 4.02 | (2) Whenever there is an interruption in service, the Contractor shall inform the Government Contracting Officer’s Representative (COR) of the estimated time that the system or data will be unavailable. The estimated timeframe for recovery of the service shall be related to the FIPS 199 system categorization for the availability of the system and if specified, agreed upon service level agreements (SLA) and system availability requirements. The Contractor shall provide regular updates to the Government Contracting Officer’s Representative (COR) on the status of returning the service to an operating state according to the agreed upon SLAs and system availability requirements. |
| Asset Availability | 4.30 | (3) The Contractor shall maintain and ensure continued compatibility and interoperability with the Government’s systems, infrastructure, and processes outlined within the Functional Requirement Document (FRD) for the term of the contract. In the event of an unavoidable compatibility and interoperability issue, the Contractor shall provide timely notification to the Government Contracting Officer’s’ Representative (COR) and work with the Government to identify appropriate remedies and facilitate a smooth and seamless transition to an alternative solution and/or provider. |
| Banner | 5.01 | The Standard Mandatory DoD Notice and Consent Banner shall be displayed at log on to all DoD information systems. The Contractor shall choose either banner a or b based on the character limitations imposed by the system. The formatting of these documents, to include the exact spacing between paragraphs, shall be maintained. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating “OK.” |
| Banner | 5.02 | a. [Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters.] |
| Banner | 5.03 | You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. |

|  |  |  |
| --- | --- | --- |
| Banner | 5.04 | By using this IS (which includes any device attached to this IS), you consent to the following conditions: |
| Banner | 5.05 | - The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations |
| Banner | 5.06 | - At any time, the USG may inspect and seize data stored on this IS |
| Banner | 5.07 | - Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. |
| Banner | 5.08 | - This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. |
| Banner | 5.09 | - Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. |
| Banner | 5.10 | OK |
| Banner | 5.11 | b. [For Blackberries and other PDAs/PEDs with severe character limitations:] |
| Banner | 5.12 | I've read & consent to terms in IS user agreement. |
|  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MISUSE OF GOVERNMENT DATA AND METADATA | | 6.02 | (2) The Contractor shall use Government-related data only to manage the operational environment that supports the government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer. | |
| MISUSE OF GOVERNMENT DATA AND METADATA | | 6.03 | (3) A breach of the obligations or restrictions set forth in (b)(1) and (b)(2) may subject the Contractor to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and any other appropriate remedies by any party adversely affected by the breach. | |
| CONTINUOUS MONITORING | | 7.01 | The Contractor shall provide all reports required to be completed; including self- assessments required by the [FedRAMP Continuous Monitoring Strategy Guide](https://www.fedramp.gov/provide-public-comment/fedramp-continuous-monitoring-reporting-and-poam-template/) to the Government designated security point of contact (POC). In addition, the Government may request additional reports based on data required to be collected by FedRAMP’s continuous monitoring requirements. If requested, the Contractor shall provide the report to the Government Contracting Officer’s Representative (COR) within 10 business days. | |
| USE OF SUBCONTRACTORS | 11.01 | | The Contractor shall retain operational configuration and control of data repository systems used to process and store government data to include any or remote work. The Contractor shall not subcontract for the operational configuration and control of any government data. |

|  |  |  |
| --- | --- | --- |
| Location of Data | 14.01 | (1) The Contractor shall maintain all data within the United States, Territories and Possessions, which means the 50 States, the District of Columbia, and outlying areas. |
| Location of Data |  | (2) The Contractor shall provide the Government with a list of the physical locations which may contain government data within 20 calendar days of award. The Contractor and or subcontractor will provide the Government Contracting Officer’s Representative (COR) with a Physical Location report on a quarterly basis or as requested by the Government. In the event the physical location of Government data location changes, the Contractor or subcontractor shall provide written notification the Government Contracting Officer within 48 hours of the change occurring. |
| LAW ENFORCEMENT | 15.01 | (1) The Contractor shall record all physical access to the cloud storage facilities and all logical access to the government data as specified in the Schedule. This shall include the entrant’s name, role, purpose, account identification, entry and exit time. Such records shall be provided to the Contracting Officer or designee in accordance with the Schedule or upon request to comply with federal authorities. |
| LAW ENFORCEMENT | 15.02 | (2) As specified by the Contracting Officer, the Contractor shall provide immediate access to all Government data and Government-related data impacting Government data for review, scan, or conduct of a forensic evaluation and physical access to any contractor facility with Government data. If the Government data is co-located with non-Government data, the Contractor shall isolate the Government data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized Government personnel identified by the Contracting Officer, and without the Contractor’s involvement. |

|  |  |  |  |
| --- | --- | --- | --- |
| 16.01 | The Contractor shall be responsible for all patching and vulnerability management (PVM) of software and other systems’ components supporting services provided under this agreement so as to prevent proactively the exploitation of IT vulnerabilities that may exist within the Contractor’s operating environment. Such patching and vulnerability management shall meet the requirements and recommendations of NIST SP 800-40, as amended, with special emphasis on assuring that the vendor’s PVM systems and programs apply standardized configurations with automated continuous monitoring of the same to assess and mitigate risks associated with known and unknown IT vulnerabilities in the Contractor’s operating environment. Furthermore, the Contractor shall apply standardized and automated acceptable versioning control systems that use a centralized model to capture, store, and authorize all software development control functions on a shared device that is accessible to all developers authorized to revise software supporting the services provided under this agreement. Such versioning control systems shall be configured and maintained so as to assure all software products deployed in the Contractor’s operating environment and serving the Government are compatible with existing systems and architecture of the Government as outlined within the Capabilities Design Document (CDD). | | |
|  |  | | |
| Records | | 18.01 | (1) The Contractor shall provide the Contracting Officer all Government data and Government-related data in the format specified in the Schedule or as directed by the Contracting Officer. | |

|  |  |  |
| --- | --- | --- |
| Records | 18.02 | (2) The Contractor shall dispose of Government data and Government-related data in accordance with the Schedule and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures. |
| Records | 18.03 | (3) The Contracting Officer may at any time issue a hold notification in writing to the Contractor. At such time, the Contractor may not dispose of any Government data or Government-related data described in the hold notification until such time as the Contractor is notified in writing by the Contracting Officer, and shall preserve all such data in accordance with agency instructions. |
| Records | 18.04 | (4) The Contractor shall provide to the Contracting Officer within 10 business days of receipt of any requests from a third party for Government-related data. |
| Records | 18.05 | (5) When the Government is using a Contractor’s software, the Contractor shall provide the agency with access and the ability to search, retrieve, and produce Government data in a standard commercial format. |
| Spillage | 19.01 | (1) Upon written notification by the Government Contracting Officer’s Representative (COR) of a spillage, the Contractor shall coordinate immediately with the responsible Government official to correct the spillage in compliance with agency- specific instructions. |
| Spillage | 19.02 | (2) If the Contractor incurs additional cost to correct the spillage, or the effort to correct the spillage causes a delay in the performance of any part of the work under this contract, and such costs or delays were not caused by any act or omission of the Contractor, an equitable adjustment shall be made under this clause and the contract modified in writing accordingly. |
| Spillage | 19.03 | (3) No request by the Contractor for an equitable adjustment to the contract under this clause shall be allowed, unless the Contractor has given a written notice thereof within 30 calendar days after the notification prescribed in paragraph (a) of this clause. |
| Spillage | 19.04 | (4) No request by the Contractor for an equitable adjustment to the contract due to a spillage shall be allowed if made after final payment under this contract. |

|  |  |  |
| --- | --- | --- |
| Spillage | 19.05 | (5) Any spillage of data by the Contractor into the environment hosting Government Data shall be immediately reported to the Government POC (insert POC) and the Contractor will follow the POC’s instructions to clean up the spillage at the Contractor's expense. |
| Terms of Service | 21.01 | Use FAR Clause: 52.212-4(u): The following shall supersede any language in the Contractor’s commercial terms of service: |
| Terms of Service | 21.02 | (1) Confidentiality. The Government, to the extent permitted by law and regulation, will safeguard and treat information obtained pursuant to the Contractor’s disclosure as confidential where the information has been marked “confidential” or “proprietary” by the company. To the extent permitted by law and regulation, such information will not be released by the Government to the public pursuant to a Freedom of Information Act request, 5 U.S.C. § 552, without prior notification to the Contractor. The Government may transfer documents and information provided by the Contractor to any department or agency within the Executive Branch if the information relates to matters within the organization’s jurisdiction. |
| Terms of Service | 21.03 | (2) Disputes and governing law. Any and all other terms or conditions notwithstanding, disputes arising under or relating to this contract or agreement are subject exclusively to Federal law, particularly the Contract Disputes Act of 1978, as amended (41 U.S.C. §§ 7101-7109) (the Act) and the provisions of 48 CFR subpart 33.2. Except as provided in the Act, all disputes arising under or relating to this contract shall be resolved under the clause set forth at 48 CFR 52.233-1. |
| Terms of Service | 21.04 | (3) Other legal matters. Any and all other terms or conditions notwithstanding, legal actions in which the Government is a party that do not arise under or relate to this contract or agreement shall be prosecuted under applicable Federal law in the appropriate Federal venue. |

|  |  |  |
| --- | --- | --- |
| Terms of Service | 21.05 | (4) Endorsement. The Contractor may not use the name, seal, logo or other readily identifiable indicia of any Government agency or organization in such a way that may be construed as advertising or endorsement by the Government of the Contractor. The Contractor may include within a list or display of the Contractor’s customers for the purposes of advertising or publicity the names, seals, logos or other indicia of Government agencies and organizations that have entered into contracts with the Contractor. However, it must not be stated or implied that the Government in any way recommends or endorses the products or services of the Contractor. |
| Terms of Service | 21.06 | (5) Indemnification and renewal. Any other terms or conditions notwithstanding, this contract or agreement shall not and does not require the Government to (i) indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability, which would violate the Anti- Deficiency Act (31 U.S.C. § 1341) (ADA), or (ii) automatically renew this contract or agreement at any time in the future, which would violate the ADA. Any such provisions set forth in this contract or agreement are unenforceable against the Government. |
|  |  |  |
|  | | |
| Test Readiness Review - TRR |  | * Schedule has been updated as necessary * Risks and Mitigations have been updated as necessary * All TRR exit criteria and key issues have been completed * Training material complete and delivered |

|  |  |
| --- | --- |
| Test Readiness Review - TRR | Connection approval process  Incident Response Plan (IRP) with Tactics, Techniques and Procedures (TTPs) |
| Test Readiness Review - TRR | Test and Evaluation:  '- All final Government Acceptance Test documents reviewed and approved   * No Category 1 or 2 defects * Training materials accepted and approved T&E Test Report |
| Test Readiness Review - TRR | Integrated Deployment Plan  IT service profile in the DISA OPS Service Operations Center (SOC) has been created/updated and verified by the Ops Lead for accuracy  execute order for Production environment after DRR Approval is obtained  - NRRB concurrences/Approval |

# Communications Security (COMSEC) Service

As defined in [DoDI 8560.01](http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf), COMSEC Monitoring and Information Assurance Readiness Testing, the COMSEC monitoring requirements enable the DoD to employ various measures designed to deny unauthorized persons from gaining information of value, that might be derived from the possession and study of voice, video or data communications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. The implementation of COMSEC monitoring will prevent unauthorized interceptors from accessing the system’s voice, video or data communications, while still delivering content to the intended recipients. These actions are in conjunction with the requirements to establish a system defense-in-depth architecture, continuous monitoring strategy.

The contractor shall be responsible for establishing, maintaining and documenting a COMSEC monitoring program to adequately manage, protect and control sensitive information that has been provided or generated under the contract. The contractor shall conduct annual assessments of their COMSEC monitoring program and submit annual written assessments to the KO on the anniversary month of contract award. These assessments are part of the continuous monitoring and the persistent cyber operations (PCO) requirements to ensure the security of the system.

**Deliverable:** The contractor shall provide a COMSEC Monitoring Plan (contractor determined format) thirty (30) business days after contract award to the KO and COR for acceptance. The KO 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 KO and COR an updated plan based on comments provided by the Government.

Annually, on the anniversary date of acceptance of the COMSEC Monitoring Plan, the contractor shall submit verification (i.e. Assessment report and sample assessment responses) to the KO and COR.

**Note:** This COMSEC requirements is different than the requirements outlined in section 7.4.4 of the FRD.

# 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 Plan:** 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.

**Deliverable:**

The contractor shall provide a Cyber Threat Security Plan (contractor determined format) thirty (30) business days after contract award to the KO and COR for acceptance. The KO 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 KO 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 KO and COR that the Plan remains valid.

# 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 DISA in completing the PIA, the contractor shall provide DISA with all relevant information and data in the form and quality required for completion. Annually, on the anniversary date of acceptance of the DLPCM Plan, the contractor shall submit verification to the KO and COR that the Plan remains valid.

**Deliverable:**

The contractor shall provide a DLPCM Plan (contractor determined format) sixty (60) business days after contract award to the KO and COR for acceptance. The KO 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 KO 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 KO and COR that the plan remains valid.

# Transition and Decommission

The contractor shall provide Transition and Decommissioning Plan (contractor determined format) that provide 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 contractor shall provide a Transition and Decommissioning Plan (Contractor determined format) sixty (60) business days after contract award to the KO and COR for acceptance. The KO and COR have ten (10) business days to provide written acceptance or feedback to the contractor. If no written acceptance is received within the 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 KO and COR an updated plan based on comments provided by the Government.

Annually, on the anniversary date of acceptance of the Transition and Decommission Plan, the contractor shall submit verification to the KO and COR that the Plan remains valid.

# Supply Chain Risk Management (SCRM)

Section 5.18 of the DoD CC SRG outlined the SCRM 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. 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 contractor shall provide an updated SCRM Plan (contractor determined format) to the COR and Program Manager (PM) 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 Cloud Service Provider conforms to the applicable Revised 508 Standards. The Cloud Service Provider must state tasks to meet section 508 accessibility in the PWS (attachment 04).

**Deliverable:** The CSP shall use the GSA 508 Voluntary Product Accessibility Template (VPAT) to provide the Government with an updated copy of the VPAT report within twenty (20) business days after contract award. 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 contract 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).