DEFENSE ADVANCED RESEARCH PROJECTS AGENCY MISSION SERVICES OFFICE UNCLASSIFIED INFORMATION TECHNOLOGY DIRECTORATE SERVICES AND SUPPORT

1 PROJECT TITLE:

Defense Advanced Research Projects Agency (DARPA) Mission Services Office (MSO) Unclassified Information Technology Directorate (ITD) services and support

2 BACKGROUND:

This is a performance work statement (PWS) for unclassified information technology (IT) services and support for DARPA. DARPA is located at 675 North Randolph Street, Arlington, VA 22203-1714. A disaster restoration site is located at (b)(1) (b)(1) and is considered part of the enclave.

The DARPA mission is to maintain U.S. technological superiority over potential adversaries by identifying and supporting breakthrough technologies of interest to the Military. IT services and support required to meet this responsibility include "state-of-the-shelf" (newest available) tools and services, and rapid, flexible responses to mission-essential and evolving government requirements. The MSO of DARPA will oversee this task order. In support of DARPA's mission, the contractor shall provide the services as detailed in this PWS across the defined functional areas.

The contractor shall provide and manage the entire range of IT services, support, and infrastructure necessary to implement the DARPA IT operational objectives, which are expected to evolve over the course of this task order. DARPA envisions that the government staff will focus on inherently governmental functions to include articulating mission requirements to the contractor, strategic planning, capital planning, information assurance (IA) policy and oversight, verification and validation, and performance monitoring. DARPA may use other government or commercial third parties to advise and/or assist in performing its responsibilities. DARPA, being a Department of Defense (DoD) organization, must comply with its risk management framework (RMF) in order to operate. Therefore, DARPA prescribes to an iterative lifecycle for all services to be provided by the contractor. The DARPA services lifecycle will be an ongoing process of continual improvement, "state-of-the-shelf" products, initial assessments and re-assessments of the security posture, and compliance of all services to ensure that DARPA networks maintain their authority to operate (ATO). DARPA also anticipates a realization of cost savings and cost effectiveness due to continuous improvement efforts by the contractor.

IT services provided under this PWS are essential to the accomplishment of DARPA's mission. DARPA is a multi-platform environment. It is critical that continuity of operations and services be maintained at the current full performance level during the period of transition from the incumbent contractor to the successful Offeror. To minimize the risk inherent in transition, DARPA will proactively facilitate the transfer of explicit and tacit knowledge, methods, and procedures from the DARPA staff and the incumbent contractor staff to the successful Offeror. To create an environment for successful transition, DARPA envisions that this PWS will be accomplished in a manner that provides an orderly 'ramp up' for the successful contractor and an orderly 'ramp down' for the incumbent contractor.

3 SCOPE:

This PWS establishes the basic requirements related to providing office computing, networking, communications service, design and development, and technical support services to DARPA. The work includes seven primary unclassified functional task areas which are: (1) Program Management; (2) Infrastructure Services including Intranet/Extranet Support, Network Access, LAN Services and Connectivity, Capacity Management, and Network Hardware Management and Maintenance; (3) Operational Support including Server Operating System, E-mail, Fax and Print, Access Management, Backup and Restore, Database, Help Desk, User Training, Software Suite, and Application Support, etc.; (4) Professional Services; (5) Analysis and Requirements Services; (6) Software Development, Maintenance, and SharePoint Services; and (7) Information Assurance and Network Defense Services. Work identified in this document shall meet the levels of service specified in the service level objectives (SLOs). Services in this task order are "24 x 7 x 365," however, the predominant amount of service tickets are generated during DARPA's core hours between 7am and 7pm, Monday through Friday. All DARPA information resources and contractor-generated data such as system log data, documentation, program code, automated scripts, and ancillary information under the task order is owned by the Government. As such, the contractor must allow and provide capabilities for authorized government managers and staff, as well as designated contractors, access to such data. Upon request by the Government, the contractor shall, without delay, deliver and convey any/all requested DARPA files/documents, etc. to the appropriate DARPA person or organization. Likewise, the contractor must provide on-going direct systems/automated access to DARPA files and databases. Such direct systems access shall include administrative or root type access for the purpose of oversight, generating reports, forensics, and analysis. Management consoles must be accessible for validation/monitoring purposes. Deliverables required by the task order are government property and may be redistributed within the Agency for management or verification purposes.

A current list of government-furnished equipment (GFE) will be provided at award and will be attached to the task order. Additional and replacement IT equipment necessary to perform the duties throughout the period of performance of this task order will be procured through this task order and provided back to the contractor as GFE. The contractor will manage the government property accountable under this task order. DARPA will provide government-furnished space which includes all furniture, equipment, telephone services, office supplies, etc. needed for the performance of this task order.

4 APPLICABLE DOCUMENTS: DEFINITIONS AND REFERENCES:

4.1 Definitions

For the purposes of this document, the following definitions apply:

Access Management helps to protect the confidentiality, integrity, and availability of assets by ensuring that only authorized users are able to access or modify the assets. Access management is sometimes referred to as "rights management" or "identity management."
Accredited means that a system or facility has been granted ATO by the authoring official (AO) of a government agency or entity and/or the Director, Security and Intelligence, DARPA, based on accreditation requirements specified by appropriate DoD 8500-series documents.
Activity refers to a set of actions designed to achieve a particular result.
Activities are usually defined as part of processes or plans, and are documented in procedures.

Asset refers to any hardware, software, or service capability. Assets of a service provider include anything that could contribute to the delivery of a service.
Availability refers to the ability of a configuration item or IT Service to perform its function when required. Availability is usually calculated as a percentage based on agreed service time and downtime.
Bundle refers to the combination of selected hardware, software, and support services used to create a service delivery point.
Capacity refers to ubiquity of access, connectivity, redundancy/diversity, compute capacity, committed information rate/peak information rate, and growth potential/scalability.
Change Management refers to the process responsible for controlling the lifecycle of all changes. The primary objective of change management is to enable beneficial changes to be made, with minimum disruption to IT services.
Closure refers to the act of changing the status of an incident or service request to the final status in its lifecycle. When the status is "closed," no further action is taken.
Closure Time refers to the act of closing a user request (a.k.a. Help Desk ticket) which will occur after the request has been completed to the user's satisfaction and a Help Desk manager has reviewed and agreed that the request has been resolved.
Configuration Control Board (CCB) refers to the government and contractor representatives who recommend approval or disapproval of proposed engineering changes to a configuration change or modification.
Configuration Item (CI) refers to any unclassified component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by configuration management. CIs are under the control of change management. CIs typically include IT services, hardware, software, buildings, people, and formal documentation such as process documentation and SLOs.
Configuration Management refers to the process responsible for maintaining information about CIs delivering an IT service, including their relationships to other CIs. This information is managed throughout the lifecycle of the CI.
Contractor refers to an entity in private industry that enters into contracts/task orders with the Government to provide goods or services.
Continuity of Operations (COOP) Site refers to the site (currently located at (b)(1) (b)(1) capable of providing failover capability in the event that the building at Founders Square (Arlington, VA) becomes unavailable.
Core Hours are DARPA's standard business hours which are 7am to 7pm, Monday through Friday, local time, excluding federal holidays.
DARPA Enclave, for the purposes of this task order, refers to 675 North Randolph St., (b)(1) Arlington, VA and
DARPA Personnel refers to both government and contractor personnel on-site at DARPA.
DARPA Portal refers to the intranet site providing DARPA news, information, and services.
DARPA Public Network (DPN)/DPN.org refers to the separate unclassified network designed specifically to allow DARPA personnel to connect to universities and other institutions with fewer restrictions than on the DARPA Management Services System.
DARPA Store Front refers to an online, user-friendly, interface to the service catalog allowing users to 'purchase' services.

Demand Management refers to activities that understand and influence government demand for services and the provision of capacity to meet these demands. At a strategic level, demand management can involve analysis of patterns of business activity and user profiles.
DARPA Management Services System (DMSS) is the primary unclassified data network.
DoD Directive 8570 is the DoD directive that describes the certification requirements for individuals working on security or security-related functions. Note: most services under this effort have security-related functions.
E-Mail refers to a widely used network application in which electronic mail messages are transmitted between end users over various types of networks using a variety of network protocols.
Event refers to a change of state which has significance for the management of a CI or IT service. The term is also used to mean an alert or notification created by any IT service, CI, or monitoring tool. Events typically require IT operations personnel to take actions, and often lead to incidents being logged.
Failure refers to the loss of ability to operate to specification, or to deliver the required output. The term may be used when referring to IT services, processes, activities, CIs, etc. A failure often causes an incident.
Founders Square refers to the area on Wilson Boulevard between Quincy Street and North Randolph Street in Arlington, VA where DARPA is located.
Governance refers to the act of ensuring policies and strategy are actually implemented, and that required processes are correctly followed. Governance includes defining roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.
Government refers to the person or group who receives the hardware, software, and related services provided under this PWS, in this case, the MSO, and defines the SLOs. The term is also sometimes informally used to mean users, for example "this is a government-focused organization."
Government Survey is the primary means for assessing levels of government satisfaction.
Help Desk Ticket refers to user support requests and falls into four ticket types: Security Incident, Incident, Service Requests, and Move, Add, Change, and Delete (MACD).
Incident refers to an unplanned interruption to an IT service or a reduction in the quality of an IT service. Failure of a CI that has not yet impacted service is also an incident. Incidents prohibit a user's ability to do his or her job (e.g. a user's network drop is not working).
IT Service refers to a service provided to one or more customers by an IT service provider. An IT service is based on the use of IT and supports the Government's business processes. It is composed of a combination of people, processes, and technology.
Key Personnel refers to those persons who are essential to work performance of the task order. All candidates to replace positions designated as key personnel in the task order, or candidates for newly designated or created key personnel positions, shall only be utilized under the task order with government concurrence. The contractor shall provide the resumes for candidates for positions designated as key personnel to the Government for government review and concurrence and the candidates shall meet with the Government as part of the oversight process. In the event that key personnel performing under the task order are to be replaced at the election of the contractor, 30 days advance written notice of the replacement shall be provided to the Government. The contractor shall provide notice to the Government as soon as practicable in the event that key personnel are unable to perform under the task order for a period of two weeks or more, terminate their employment with the contractor, or provide notice to the contractor of their

intent to terminate employment with the contractor. The Government can request replacement of key personnel at any time.

Local Area Network (LAN) refers to the internal unclassified computer network that currently supports the DARPA enclave.

Legacy refers to hardware, software, or application systems currently in use in the DARPA enclave.

Move, Add, Change, and Delete (MACD) refers to a request for a change to a CI.

Offsite Storage means a location of sufficient distance (at least 10 miles) from the DARPA enclave to assure survival of the material in case of disaster or emergency events. Note: this is in addition to the (b)(1) site.

Operational Level Agreement (OLA) defines the interdependent relationships among the internal groups of DARPA. The agreement describes the responsibilities of each internal support group toward other support groups, including the process and timeframe for delivery of their services. The objective of an OLA is to present a clear, concise and measurable description of the service provider's internal support relationships. Copies of the OLAs will be provided to the contractor at task order award.

Plan of Action and Milestones (POA&M) refers to a document that identifies tasks needing to be accomplished to complete a project. It details resources required to accomplish the elements of the project, any milestones in meeting the tasks, and scheduled completion dates for the milestones. Typically, the contractor will provide a recommended POA&M for contracting officer's representative (COR) approval.

Privileged User refers to users who have system rights beyond those of a basic user.

Problem refers to the cause of one or more incidents. The cause is not usually known at the time that the problem record is created.

Professional Services Project refers to a task undertaken to meet specific goals and objectives that has a definable beginning and end. In respect to this task order, it is to provide one-time or first-time products or services. In the case of a first-time project, the intent is that once completed, a product or project will become a repeatable service or product that will be added to the Service Catalog and made available to DARPA Users via the DARPA Store Front.

Project Request (PR) refers to the initial request from the Government to the contractor defining the requirements of the work to be completed by the Professional Services staff.

Project Change Request (PCR) refers to the request, by the Government or contractor, to change the scope of a given project.

Resolution refers to an action taken to repair the root cause of an incident, or to implement a workaround. If a workaround is implemented, a new problem record is created to identify the root cause. Resolution time is when the user responds that he or she agrees that the service request or incident has been resolved. If a user does not respond within two business days of reasonable attempts to contact, it will be assumed that the user agrees, and the ticket can be resolved.

Responsiveness is a measurement of the time taken to respond to a security incident, service request, etc.

Retired Services refers to services that have been removed from the Service Catalog and are no longer available.

Security Features refers to the security features that are directed by DoD- or federal-government-mandated guidance, law, or regulation, or as determined by DARPA. Where questions of the interpretation of requirements are necessary, the Government will consult with the contractor but shall be the final arbiter.

Security Incident refers to an assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Service Asset refers to any capability or resource of a service provider. A service asset comprises the hardware which, when bundled with software and security features (e.g. smart card technology), is necessary for DARPA users to perform computing functions, to access computing resources, and to receive the government IT services described in this PWS.
Service Catalog refers to a database or structured document with information about all available IT services. The Service Catalog is the only part of the service portfolio available for deployment. The Service Catalog includes information about deliverables, prices, contact points, and ordering processes.
Service Delivery Maturity refers to the frameworks and quality models such as ISO9000, ISO20000, the IT Infrastructure Library (ITIL), Capability Maturity Model (CMM), and Capability Maturity Model Integration (CMMI) and provides a blueprint and a road map for improving processes and procedures. Each framework and quality model has specific strengths in helping meet business goals, including the potential for cost reductions, increased customer satisfaction, and greater productivity.
Service Delivery Points (SDP) refers to customer-facing, hardware CIs. This includes desktops, laptops, tablets, personal digital assistants (PDAs), cellular, satellite, and landline Voice over Internet Protocol (VoIP) phones, printers, copiers, and all devices which may be added to, replace, or supplement any of the above devices during the course of the task order.
Service Level Management (SLM) refers to the process responsible for negotiating the levels of service to be provided, and ensuring that these are met**.**
Service Level Objective (SLO) is a specified level of service included as part of the PWS. SLOs are a means of measuring the performance of the service provider and are outlined as a way of communicating the Government's requirements between the two parties.
Service Provider refers to an organization supplying services to the Government. "Service provider" is often used as an abbreviation for "IT service provider."
Service Request refers to a request from a user for information, advice, or a pre-approved change that is low risk, relatively common, and follows standard procedures. The nature of a service request does not prohibit a user's ability to perform his or her job (e.g., a user cannot open an e-mail attachment, but can still send and receive e-mails).
State-of-the-Shelf refers to the innovative use of proven/stable technologies vs. leading/bleeding edge.
Test Bed refers to the stand-alone network environment simulating the DMSS used to test and evaluate new and modified technologies and applications.
Underpinning Contract refers to a contract between the awardee and a third party. The third party provides goods or services that support delivery of an IT service to the Government; for example, contracts with the internet service provider and the copier vendor. The underpinning contract defines targets and responsibilities that are required to meet agreed SLOs.
Unified Communication (UC) refers to the integration of real-time communication services such as instant messaging (chat), presence information, telephony (including Internet Protocol (IP) telephony), video conferencing, call control, and speech recognition with non-real-time communication services such as unified messaging (integrated voicemail, e-mail, Short Message

Service (SMS), and fax). UC is not a single product, but a set of products that provides a consistent unified user interface and user experience across multiple devices and media types.
User refers to an individual person or system process acting on behalf of an individual person authorized to access an information system.
User Account refers to authorized access to use specified services, exclusive of the hardware and LAN drop.
WWW.DARPA.MIL refers to the external, public-facing DARPA web site.

4.2 References

(a) DoD Directive 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," current edition
(b) DoD Directive 5015.02-STD, "Electronic Records Management Software Applications Design Criteria Standard," current edition
(c) DoD Directive 8100.02, "Use of Commercial Wireless Devices, Services and Technologies," current edition
(d) DoD Directive 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," current edition
(e) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT) ," current edition
(f) DoD Directive O-8530.1, "Computer Network Defense (CND)," current edition
(g) DoD Directive 8570.01, "Information Assurance Training, Certification and Workforce Management," current edition
(h) DoD 5200.01, "DoD Information Security Program: Overview, Classification, and Declassification," current edition
(i) DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)," current edition
(j) CJCSI 6510.01F, "Information Assurance (IA) and Computer Network Defense (CND) ," current edition
(k) DoD STIGs, "Security Technical Implementation Guides", comprehensive list, http://iase.disa.mil/stigs/stig/index.html
(l) NSA/CSS Information Assurance Directorate CGS, "Decommission Capability v1.1.1," current edition
(m) Memorandum for CIOs of Executive Departments and Agencies, "Transition to IPv6," current edition
(n) "DoD IPv6 Standard Profiles for IPv6 Capable Products v5.0," current edition
(o) DoD Approved Software, Enterprise Software Initiative, http://www.esi.mil/
(p) Clinger-Cohen Act of 1996, Public Law 104-106, 40 U.S.C. 25.
(q) Inventory Reform Act of 1998, Public Law 105-270, 31 U.S.C. 501 note.
(r) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," current edition
(s) Rehabilitation Act of 1973, Section 508, as amended (29 U.S.C. 794d), current edition
(t) DoD Directive 3020.26, Department of Defense Continuity Programs, current edition
(u) DoD Enterprise Directory Services Capability Document, Version 2.0, current edition
(v) Section 552a of title 5, United States Code, the Privacy Act of 1974
(w) DoD Directive 5400.11-R, "DoD Privacy Program," current edition
(x) ASD Memo, "Disposition of Unclassified DoD Computer Hard Drives

Memorandum," current edition
(y) DoD Instruction 8500.01, "Cybersecurity," current edition
(z) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," current edition

4.3 Service Level Objectives

This section provides Service Level Objectives (SLOs) and associated performance metrics for key IT service management processes and functional area tasks defined in the PWS. SLOs define quantitative measurements of performance over time, and establish the contractual understanding of the Government's service expectations and the contractor's commitment to meeting these expectations.

The contractor shall provide written, monthly reports regarding compliance with all SLOs specified in this PWS. Performance of the contractor against all SLOs is auditable by the Government or a third party on behalf of the Government. The contractor shall implement measurement and monitoring tools to produce the reports necessary to measure its performance as specified by the SLOs. Upon request in connection with an audit, and at no additional charge to the Government, the contractor shall provide the Government with information and access to tools and procedures used to produce such metrics.

The SLOs and PWS requirements will be reviewed and adjusted as necessary, annually on the anniversary of the task order, to meet changing IT service and support requirements. Adjustments to SLOs during the annual review will be made by mutual agreement between the Government and the contractor and any costs associated with those adjustments will be addressed.

4.3.1 Standard Exceptions:

Standard Exceptions applicable to all SLOs are the following:

a. Contracting Officer's Representative (COR) waiver
b. COR-approved, scheduled maintenance and scheduled downtime (in some cases)
c. Any networks or network equipment not owned or controlled by the contractor
d. Circumstances beyond reasonable control of the contractor, including, without limitation, acts of war, insurrection, armed conflict, embargo, fire, flood, or power outages. Power outages that do not affect service availability due to redundant capabilities are excluded.
e. Any negligence, willful misconduct, or use of services by DARPA personnel in breach of DARPA's Acceptable Use Policy.

4.3.2 List of Service Level Objectives

SLOs are defined across eight service and support categories, as follows:

1. Service Delivery
1.1 Configuration Item Fulfillment Resolution Time
1.2 Configuration Item Procurement Resolution Time
1.3 E-mailed Service Request Responsiveness
1.4 Service Request "End-to-End" Closure Time
1.5 File Restoration Request Closure Time
1.6 Reopened Ticket Percentage
1.7 Configuration Item Fulfillment Resolution Time (Infrastructure item/non-Customer-facing)

2. Service Availability
2.1 LAN Infrastructure Availability
2.2 Internet Availability
2.3 Virtual Private Network Availability
2.4 Infrastructure Servers Availability
2.5 E-mail Services Availability
2.6 Server Services Availability
2.7 Telephone Services Availability
2.8 Video Teleconferencing Availability
2.9 Total Scheduled Downtime
2.10 Internal Web Services
2.11 DARPA Public Network (DPN) Availability

3. Incident Management
3.1 Network Incident Responsiveness
3.2 Network Incident Resolution Time

4. Security Management Services
4.1 Computer Security Incident Responsiveness
4.2 Vulnerability Announcement Mitigation Distribution Timeliness
4.3 Vulnerability Announcement Mitigation Compliance Percentage
4.4 Other DoD-Directed Actions Timeliness

5. Asset and Configuration Management
5.1 Asset / Inventory Accuracy
5.2 Asset Tracking Database Update Timeliness
5.3 Software Update / Upgrade Timeliness

6. User Satisfaction
6.1 User Satisfaction Survey Results
6.2 Operational Level Agreement Compliance
6.3 First Contact Resolution Percentage

7. Professional Services Performance
7.1 Projects Completed On-Time
7.2 Projects Completed Within Budget

8. Program Management Performance
8.1 Reporting Timeliness and Accuracy
8.2 Contractor Availability and Responsiveness
8.3 Upgrades Currency and Maintenance

4.3.3 Individual SLO Descriptions

The following pages detail each SLO including its description, performance target, exceptions, measurement method, data sources, and calculation formula. Time-based performance targets are considered "less than or equal to." Percentage-based targets are considered the minimum performance level. Performance measurement calculations associated with the SLOs will result in a determination of "Pass" or "Fail" for each SLO on a monthly basis. Contractor shall make

every effort with customers (using email, phone call, SETA support, etc.) to set appointment times for work/delivery.

Service Delivery

SLO Number	1.1
SLO Category	Service Delivery
SLO Title	**Configuration Item Fulfillment Resolution Time**
SLO Description	Time to complete an install, move, add, change, and delete (MACD), or de-installation of a standard Configuration Item from inventory after a Government approved request is received. This metric is from the initial request until successful completion of the MACD. Includes time to create accounts/permissions, and install, configure and test new hardware or software.
Time Applicability	Core Hours
Exceptions and Exclusions	Standard Exceptions; Does not include time to obtain the requisite approvals, schedule an agreed upon time for the work to take place, verify completion of services and confirm satisfaction, or while a User is unavailable for delivery of services. Infrastructure items/non-Customer-facing (SLO 1.7).
Performance Target	≤ 2 business days (excludes VoIP phones)
Measurement Window	Monthly
Measurement Method	End-to-end elapsed time (business days)
Data Sources	Help Desk Management System (raw ticket data)
Calculation Formula	Average Completion Time for Applicable Requests (total time/# tickets)
Additional Requirements	
Related PWS section(s)	Sec. 5.6.3.41 Request Fulfillment, Sec. 5.6.3.42 Moves, Adds, Changes, and Deletes (MACDs)

SLO Number	1.2
SLO Category	Service Delivery
SLO Title	**Configuration Item Procurement Resolution Time**
SLO Description	Time to procure a Configuration Item from a vendor after a Government approved procurement request/order is received. This is the elapsed time from ordering Configuration Items to receiving them into inventory (i.e., does not include delivery/installation at User site, which is covered by SLO 1.1; See Exceptions and Exclusions below).
Time Applicability	Core Hours
Exceptions and Exclusions	Standard Exceptions; Does not include time to obtain the requisite approvals, previously agreed upon vendor lead times for infrastructure CIs or to perform fulfillment / MACDs (see SLO 1.1).
Performance Target	≤ 5 business days for user-requested purchases. For all other purchases, procurement should be according to established project plan or Government-approval.
Measurement Window	Monthly
Measurement Method	End-to-end elapsed time (business days)
Data Sources	Help Desk Management System (raw ticket data)
Calculation Formula	Average Completion Time for Applicable Requests (total time/# tickets)
Additional Requirements	
Related PWS section(s)	Sec. 5.6.3.44 Service Catalog – DARPA Store Front Sec. 5.6.3.44 Service Catalog / Store Front

SLO Number	1.3
SLO Category	Service Delivery
SLO Title	**E-mailed Service Request Responsiveness**
SLO Description	Time to acknowledge (via email or phone call) an e-mailed Help Desk request. The response shall indicate that the Help Desk is aware of the request and provide an estimated time for service delivery.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions
Performance Target	a. Core hours: ≤ 30 minutes b. Non-Core hours: ≤ 60 minutes
Measurement Window	Monthly
Measurement Method	Elapsed time from receipt of e-mail to issuing reply to originator
Data Sources	Help Desk Management System (raw ticket data); E-mail Messaging system
Calculation Formula	Average Response Time for Applicable Requests (total time/# tickets)
Additional Requirements	*E-mail transactions to the Help Desk shall result in a reply e-mail and phone call to the originating User*
Related PWS section(s)	Sec. 5.6.3.28 Help Desk Services

SLO Number	1.4
SLO Category	Service Delivery
SLO Title	**Service Request "End-to-End" Closure Time**
SLO Description	Time to resolve a Service Request to the User's satisfaction from the receipt of the initial request by the Help Desk. This is an "end-to-end" metric inclusive of the entire process from initial contact, across any support tier, until final closure of the request.
Time Applicability	Core Hours
Exceptions and Exclusions	Standard Exceptions; Excludes Configuration Item fulfillment/MACDs (SLO 1.1) and procurement requests (SLO 1.2).
Performance Targets	a. VIP ≤ 30 minutes b. Service Outage Tickets: ≤ 60 minutes c. Routine Tickets: ≤ 4 hours d. All other Tickets: ≤ 2 business days
Measurement Window	Monthly
Measurement Method	End-to-end elapsed time
Data Sources	Help Desk Management System (raw ticket data)
Calculation Formula	Average Closure Time using interior mean, which will exclude one percent of tickets with the longest resolution time, and one percent of tickets with the shortest resolution time.
Additional Requirements	*A list of VIPs will be provided to the contractor. For the purposes of this SLO, a Service Outage Ticket is defined as a localized event or issue that creates a work stoppage for the customer. Routine tickets are those that do not require escalation beyond the help desk (Tiers 1 and 2)*
Related PWS section(s)	Sec. 5.6.3.27 contractor Service Level Support Sec. 5.6.3.28 Help Desk Services Request Fulfillment Sec. 5.6.3.41 Request Fulfillment

SLO Number	1.5
SLO Category	Service Delivery
SLO Title	**File Restoration Request Closure Time**
SLO Description	Time to restore a file to the User's satisfaction from the receipt of the initial restore request by the Help Desk. This is an "end-to-end" metric inclusive of the entire process from initial contact, across any support tier, until final closure of the request. Also assumes that the User can accurately define the file(s) for restoration.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions
Performance Targets	a. Successfully restore file from on-line backups: ≤ 2 hours b. Successfully restore file from off-line/on-site archive: ≤ 24 hours c. Successfully restore file from off-site archives: ≤ 5 business days
Measurement Window	Monthly
Measurement Method	End-to-end elapsed time
Data Sources	Help Desk Management System (raw ticket data); Backup/ Restore Logs
Calculation Formula	Average Completion Time
Additional Requirements	
Related PWS section(s)	Sec. 5.6. 3.15 Backup and Restore Services Sec 5.6.3.28 Help Desk Services

SLO Number	1.6
SLO Category	Service Delivery
SLO Title	**Reopened Ticket Percentage**
SLO Description	The proportion of Service Requests that require tickets to be re-opened to complete resolution.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions
Performance Targets	≤ 1% Tickets re-opened
Measurement Window	Monthly
Measurement Method	Repeat Incidents that were not resolved the first time
Data Sources	Help Desk Management System (raw ticket data); Problem Management System
Calculation Formula	Repeat Incidents / Total Incidents * 100
Additional Requirements	
Related PWS section(s)	Sec 5.6.3.28 Help Desk Services

SLO Number	1.7
SLO Category	Service Delivery
SLO Title	**Configuration Item Fulfillment Resolution Time (Infrastructure item/non-Customer-facing)**
SLO Description	Time to complete an install, move, add, change, and delete (MACD) or de-installation of a standard Configuration Item from inventory after a Government approved request is received. This metric is from the initial request until successful completion of the MACD. Includes time to create accounts/permissions, and install, configure and test new hardware or software.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions - Does not include time to obtain the requisite approvals, schedule an agreed upon time for the work to take place, verify completion of services and confirm satisfaction, or while a User is unavailable for delivery of services. Customer-facing items (SLO 1.1).
Performance Targets	Per Government-approved Project Plan
Measurement Window	Monthly
Measurement Method	
Data Sources	Help Desk Management System (raw ticket data); Problem Management System
Calculation Formula	"Pass" or "Fail" based on missing the target for relevant MACDs during reporting period
Additional Requirements	
Related PWS section(s)	Sec 5.6.3.14 Service Continuity Management Sec. 5.6.2.20 Local Area Network (LAN) Communication Services Sec. 5.6.2.21 Internal (LAN) Connectivity Sec 5.6.2.29 Network Management System (NMS) Service

Service Availability

SLO Number	2.1
SLO Category	Service Availability
SLO Title	**Local Area Network Infrastructure Availability**
SLO Description	The percentage of time the DMSS Local Area Network (LAN) is fully functioning and available to Users.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions, Availability will be monitored per device and monitoring criteria cannot be aggregated and averaged to meet the SLO requirements. Outages that do not affect service availability due to redundant capabilities are excluded. Note: Failure of equipment managed by the contractor will not be excluded from the requirements of this SLO.
Performance Target	≥ 99.99%
Measurement Window	Monthly
Measurement Method	Uptime, Scheduled Downtime (SD), and Total Time in Reporting Period (TTRP)
Data Sources	Network Monitoring Applications; Incident Management System
Calculation Formula	Uptime / (TTRP – SD) * 100
Additional Requirements	
Related PWS section(s)	Sec. 5.6.3.14 Service Continuity Management Sec 5.6.2.20 Local Area Network (LAN) Communication Services Sec. 5.6.2.21 Internal (LAN) Connectivity Sec. 5.6.2.29 Network Management System (NMS) Service

SLO Number	2.2
SLO Category	Service Availability
SLO Title	**Internet Availability**
SLO Description	The percentage of time Internet access is fully functioning and available to Users.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions, Outages that do not affect service availability due to redundant capabilities are excluded. Note: Failure of equipment managed by the contractor will not be excluded from the requirements of this SLO. DPN (covered in SLO 2.11)
Performance Target	≥ 99.99%
Measurement Window	Monthly
Measurement Method	Uptime, Scheduled Downtime (SD), and Total Time in Reporting Period (TTRP)
Data Sources	Network Monitoring Applications; Incident Management System
Calculation Formula	Uptime / (TTRP – SD) * 100
Additional Requirements	
Related PWS section(s)	Sec. 5.6.3.14 Service Continuity Management Sec. 5.6.2.19 External Network Access and Services Sec. 5.6.2.29 Network Management System (NMS) Service

SLO Number	2.3
SLO Category	Service Availability
SLO Title	**Virtual Private Network Availability**
SLO Description	The percentage of time the Government Virtual Private Network (VPN) is fully functioning and available to Users.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions, Outages that do not affect service availability due to redundant capabilities are excluded. Note: Failure of equipment managed by the contractor will not be excluded from the requirements of this SLO.
Performance Target	≥ 99.99%
Measurement Window	Monthly
Measurement Method	Uptime, Scheduled Downtime (SD), and Total Time in Reporting Period (TTRP)
Data Sources	Network Monitoring Applications; Incident Management System
Calculation Formula	Uptime / (TTRP – SD) * 100
Additional Requirements	
Related PWS section(s)	Sec. 5.6.3.14 Service Continuity Management Sec. 5.6.2.24 Remote Access Services

SLO Number	2.4
SLO Category	Service Availability
SLO Title	**Infrastructure Service Availability**
SLO Description	The percentage of time the Government infrastructure services, including DNS, DHCP and Domain Controllers are fully functioning and available to Users.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions, Outages that do not affect service availability due to redundant capabilities are excluded. Note: Failure of equipment managed by the contractor will not be excluded from the requirements of this SLO.
Performance Target	≥ 99.99%
Measurement Window	Monthly
Measurement Method	Uptime, Scheduled Downtime (SD), and Total Time in Reporting Period (TTRP)
Data Sources	Network Monitoring Applications; Incident Management System
Calculation Formula	Uptime / (TTRP – SD) * 100
Additional Requirements	
Related PWS section(s)	Sec. 5.6.3.14 Service Continuity Management Sec. 5.6.2 Infrastructure Services Sec. 5.6.2.24 Remote Access

SLO Number	2.5
SLO Category	Service Availability
SLO Title	**E-mail Services Availability**
SLO Description	The percentage of time the E-mail Services are fully functioning and available to Users. E-mail services are highly critical to the communications of the DARPA organization and are therefore separated out from the standard server services.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions, Outages that do not affect service availability due to redundant capabilities are excluded. Note: Failure of equipment managed by the contractor will not be excluded from the requirements of this SLO.
Performance Target	≥ 99.99%
Measurement Window	Monthly
Measurement Method	Uptime, Scheduled Downtime (SD), and Total Time in Reporting Period (TTRP)
Data Sources	Network Monitoring Applications; Incident Management System
Calculation Formula	Uptime / (TTRP – SD) * 100
Additional Requirements	
Related PWS section(s)	Sec. 5.6.3.14 Service Continuity Management Sec 5.4 Unified Communications (E-mail) Sec. 5.6.3.1 Server Operating System Support Sec. 5.6.3.4 E-mail Services

SLO Number	2.6
SLO Category	Service Availability
SLO Title	**Server Services Availability**
SLO Description	The percentages of time the specified Services are fully functioning and available to Users. All servers are categorized by Criticality Levels (1, 2 and 3) as defined in the PWS "Service Continuity Management" section.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions, Outages that do not affect service availability due to redundant capabilities are excluded. Note: Failure of equipment managed by the contractor will not be excluded from the requirements of this SLO.
Performance Target	Server Services, as defined by Criticality Level as defined in the COOP plan: a. Mission Critical Services: ≥ 99.99% or no more than 4.32 minutes of downtime/month b. Critical Services: ≥ 99.95% or no more than 21.56 minutes of downtime/month c. Non-Critical, but Essential Services: ≥ 99.9% or no more than 43.2 minutes of downtime/month
Measurement Window	Monthly
Measurement Method	Uptime, Scheduled Downtime (SD), and Total Time in Reporting Period (TTRP)
Data Sources	Network Monitoring Applications; Incident Management System
Calculation Formula	Uptime / (TTRP – SD) * 100
Additional Requirements	
Related PWS section(s)	Sec. 5.6.3.13 Shared File Services Sec. 5.6.3.14 Service Continuity Management Sec. 5.6.3.16 Disaster Recovery Services Sec. 5.6.3.21 Web Hosting Services Sec. 5.6.2 Infrastructure Services Sec. 5.6.2.18 Intranet/Extranet Services Sec 5.6.3.1 Server Operating System Support Sec. 5.6.3.7 FAX Services

SLO Number	2.7
SLO Category	Service Availability
SLO Title	**Telephone Services Availability**
SLO Description	The percentage of time Telephone Services are fully functioning and available to Users. Includes VoIP, Chat, TDM- based PBX systems, inbound/outbound FAX services, and end-point user devices, etc.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions, Outages that do not affect service availability due to redundant capabilities are excluded. Outages affecting 10 or fewer end-point devices are excluded. Note: Failure of equipment managed by the contractor will not be excluded from the requirements of this SLO.
Performance Target	≥ 99.99%
Measurement Window	Monthly
Measurement Method	Uptime, Scheduled Downtime (SD), and Total Time in Reporting Period (TTRP)
Data Sources	Network Monitoring Applications; Incident Management System
Calculation Formula	Uptime / (TTRP – SD) * 100
Additional Requirements	
Related PWS section(s)	Sec. 5.6.3.14 Service Continuity Management Sec. 5.6.3.3 Unified Communications and Telephone Services Sec. 5.6.3.7 FAX Services

SLO Number	2.8
SLO Category	Service Availability
SLO Title	**Video Teleconferencing Availability**
SLO Description	The percentage of time Video Teleconferencing (VTC) services are fully functioning and available to Users.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions, Availability will be monitored per device and monitoring criteria cannot be aggregated and averaged to meet the SLO requirements. Outages that do not affect service availability due to redundant capabilities are excluded. Note: Failure of equipment managed by the contractor will not be excluded from the requirements of this SLO.
Performance Target	≥ 99.9%
Measurement Window	Monthly
Measurement Method	Uptime, Scheduled Downtime (SD), and Total Time in Reporting Period (TTRP)
Data Sources	Network Monitoring Applications; Incident Management System
Calculation Formula	Uptime / (TTRP – SD) * 100
Additional Requirements	
Related PWS section(s)	Sec. 5.6.3.14 Service Continuity Management Sec. 5.6.3.34 Conference Rooms (AV Equipment) Support

SLO Number	2.9
SLO Category	Service Availability
SLO Title	**Total Scheduled Downtime**
SLO Description	Total time (i.e., cumulative wall-clock minutes per month) the contractor schedules operational outages or maintenance. Includes outage of any IT service that may impact any User.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions; Also, if there is a critical threat to Government systems that has a major impact, as much advanced warning as possible will be provided to Users and the maintenance will be completed regardless of the time.
Performance Target	≤ 300 Minutes per Month
Measurement Window	Monthly
Measurement Method	Total scheduled "wall-clock" downtime per reporting period.
Data Sources	Network Monitoring Applications; Incident Management System
Calculation Formula	Total Scheduled Downtime
Additional Requirements	*Total time for scheduled outages and maintenance shall be in compliance with Government approved parameters (total planned outage time, window start time and duration). Users shall be notified of scheduled outages at least three (3) days in advance.*
Related PWS section(s)	Sec. 5.6.3.14 Service Continuity Management Sec. 5.6.2 Infrastructure Services Sec. 5.6.3 Operational Services

SLO Number	2.10
SLO Category	Service Availability
SLO Title	**Internal Web Services**
SLO Description	The percentage of time that all customer facing internal web services are available to include (but not limited to): DARPA Portal, network search, customer applications to support DARPA Office operations.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions Outages that do not affect service availability due to redundant capabilities are excluded. Note: Failure of equipment managed by the contractor will not be excluded from the requirements.
Performance Target	≥ 99.99%
Measurement Window	Monthly
Measurement Method	Availability will be monitored per service and monitoring criteria cannot be aggregated and averaged to meet the requirements.
Data Sources	Network Monitoring Applications; Incident Management System, Help Desk Tickets
Calculation Formula	Uptime / (TTRP – SD) * 100
Additional Requirements	*Total time for scheduled outages and maintenance shall be in compliance with Government approved parameters (total planned outage time, window start time and duration). Users shall be notified of scheduled outages at least three (3) days in advance.*
Related PWS section(s)	Sec. 5.6.3 Operational Services Sec. 5.6.3.14 Service Continuity Management Infrastructure Support

SLO Number	2.11
SLO Category	Service Availability
SLO Title	**DARPA Public Network (DPN) Availability**
SLO Description	The percentage of time the DPN is fully functioning and available to Users.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions, Outages that do not affect service availability due to redundant capabilities are excluded. Note: Failure of equipment managed by the contractor will not be excluded from the requirements of this SLO.
Performance Target	≥ 99.99%
Measurement Window	Monthly
Measurement Method	Uptime, Scheduled Downtime (SD), and Total Time in Reporting Period (TTRP) (e.g., 43,200 minutes for 30- day month)
Data Sources	Network Monitoring Applications; Incident Management System
Calculation Formula	Uptime / (TTRP – SD) * 100
Additional Requirements	
Related PWS section(s)	Sec. 5.6.3.14 Service Continuity Management Sec. 5.6.2.20 Local Area Network (LAN) Communication Services Sec. 5.6.2.21 Internal (LAN) Connectivity Sec. 5.6.2.29 Network Management System (NMS) Service

Incident Management

SLO Number	3.1
SLO Category	Incident Management
SLO Title	**Network Incident Responsiveness**
SLO Description	Time to notify the Government and begin mitigation (e.g., containment, remediation planning and/or resolution of anomalies) after the detection and identification of a network Incident or outage event.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions;
Performance Target	a. Network outage during Core Hours: ≤ 5 minutes for ITD, 20 minutes to notify affected customers b. Network outage during non-Core Hours: ≤ 30 min for ITD, 45 minutes to notify affected customers
Measurement Window	Monthly
Measurement Method	Government correspondence and Help Desk Management System
Data Sources	Automated Network Monitoring tool; Government notification records
Calculation Formula	"Pass" or "Fail" based on missing the target for any single Incident/ event condition during the reporting period
Additional Requirements	
Related PWS section(s)	Sec. 5.6.2.28 Availability Management Sec. 5.6.3 Operational Services

SLO Number	3.2
SLO Category	Incident Management
SLO Title	**Network Incident Resolution Time**
SLO Description	Time to resolve all Data Center and Network equipment Incidents causing an unplanned system or service outage. It includes the period of time starting when an Incident is detected, through troubleshooting and complete remediation of the Incident, whereby the service is returned to a state of normal operation within the defined timeframe. Time to Return to Service covers both hardware and software components.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions;
Performance Target	a. Severity Level 1*: ≤ 4 hours b. Severity Level 2: ≤ 8 hours c. Severity Level 3: ≤ 1 business day *As defined in Section 4.3.4 of this PWS.
Measurement Window	Monthly
Measurement Method	Elapsed Time to Return to Service per Incident (by Severity Level); Severity Levels must be assessed and captured when Incidents are logged.
Data Sources	Network Monitoring Applications and Incident Management System
Calculation Formula	Time to Return to Service / Total number of Incidents
Additional Requirements	
Related PWS section(s)	Sec. 5.6.2.28 Availability Management

Security Management Services

SLO Number	4.1
SLO Category	Security Management Services
SLO Title	**Computer Security Incident Responsiveness**
SLO Description	Time to notify the Government and begin mitigation (e.g., containment, remediation planning and/or resolution of anomalies) after the detection and identification of a Security Incident.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions
Performance Target	Government notification and actions executed in accordance with "DARPA Computer Security Incident Response Guide" procedures. Timeframes and actions vary according to the type of Security Incident and when it occurs.
Measurement Window	Monthly
Measurement Method	Government correspondence and Help Desk Management System
Data Sources	Automated Network Monitoring tool; Government notification records
Calculation Formula	"Pass" or "Fail" based on missing the target for any single Incident/ event condition during the reporting period
Additional Requirements	
Related PWS section(s)	Sec. 5.6.7.2 ITD Security Services Sec. 5.6.3 Operational Services

SLO Number	4.2
SLO Category	Security Management Services
SLO Title	**Vulnerability Announcement Mitigation Distribution Timeliness**
SLO Description	Time to distribute and successfully complete installation of DoD Vulnerabilities Announcements according to contractor proposed, Government approved POA&M, (e.g. security fixes/patches and anti-virus updates) against the target population after Vulnerability Announcements are issued and deployment commences.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions; Patching delays resulting from inaccessible equipment, such as unconnected User laptops.
Performance Target	Completed by DoD-specified Compliance Date or ≤ 30 days, whichever is less, unless otherwise directed by the Government
Measurement Window	Monthly
Measurement Method	Elapsed time to update the target population for each deployment attempt (from approval to completion)
Data Sources	Automated Patch Management System
Calculation Formula	Provided via reports issued from the automated software system.
Additional Requirements	*General DoD and DARPA IA Policies Compliance.*
Related PWS section(s)	Sec. 5.6.7 Information Assurance and Network Defense Sec. 5.6.3.19 Software Distribution and Upgrades

SLO Number	4.3
SLO Category	Security Management Services
SLO Title	**Vulnerability Announcement Mitigation Compliance Percentage**
SLO Description	Percentage of DoD issued Vulnerability Announcement Mitigations installed on unclassified systems by the DoD requested compliance date unless otherwise specified in the contractor proposed, Government approved POA&M.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions
Performance Target	Device Types: a. All Servers and network equipment/appliances: = 100% b. All Desktops: ≥ 98% c. All Laptops and other applicable mobile devices: ≥ 90%
Measurement Window	Monthly
Measurement Method	Number of Vulnerability Announcement Mitigations successfully installed
Data Sources	Vulnerability Announcement Mitigations Patch Management / scanning application
Calculation Formula	For any given Vulnerability Announcement: Number of systems on which the mitigation was successfully installed / Total number of systems affected by the Vulnerability * 100
Additional Requirements	*General DoD and DARPA IA Policies Compliance.* *While the performance target allows for some margin of error due to system inaccessibility, all mitigations must eventually reach 100% and reporting will continue until 100% compliance is achieved.*
Related PWS section(s)	Sec. 5.6.7 Information Assurance and Network Defense Sec. 5.6.3.19 Software Distribution and Upgrades

SLO Number	4.4
SLO Category	Security Management Services
SLO Title	**Other DoD Directed Actions Timeliness**
SLO Description	Time to successfully complete installation of DoD directed actions due to CTOs, IAVBs, IAVTs, STIGs, etc.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions; Government approval (e.g., POA&M, Authorizing Official (AO) exceptions, etc.) Patching delays resulting from inaccessible equipment, such as unconnected
Performance Target	Completed by DoD-specified Compliance Date, unless otherwise directed by the Government (Authorizing Official (AO) or Information Systems Security Manager (ISSM)). The contractor will coordinate with the Government for implementation of all security-related changes. Due to the potential customer impact of STIG and similar changes, the contractor will submit a recommended schedule for Government approval.
Measurement Window	Monthly; Compliance with STIG, CCRI, and CNDSP requirements will also be spot-checked.
Measurement Method	Elapsed time to update the target population for each deployment attempt (from approval to completion)
Data Sources	Automated Patch Management System
Calculation Formula	Provided via reports.
Additional Requirements	*General DoD and DARPA IA Policies Compliance*
Related PWS section(s)	Sec. 5.6.7 Information Assurance and Network Defense Sec. 5.6.3.19 Software Distribution and Upgrades

Asset and Configuration Management

SLO Number	5.1
SLO Category	Asset and Configuration Management
SLO Title	**Asset / Inventory Accuracy**
SLO Description	Percentage of accurate inventory assets based on a random sample of at least 30 applicable tickets (assumes an average of 120 tickets per month). Reflects verification that asset tag, location, responsible owner, and status are all correct. Applicable ticket types include: • Update Assets • Install Hardware • Relocate Equipment • Uninstall Hardware • Install Printer/Copier Sample selection and comparison is performed by the contractor's Quality Assurance component, and is auditable by the Government or a Government designated third-party.
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions
Performance Target	≥ 98%
Measurement Window	Monthly
Measurement Method	Number of Accurate Items, Total Items Sampled
Data Sources	Asset Tracking Database, Credit Asset Report and comparison reporting
Calculation Formula	Number of Items where data is correct / Total Items Sampled * 100
Additional Requirements	
Related PWS section(s)	Sec. 5.6.1.4 Inventory / Asset Management

SLO Number	5.2
SLO Category	Asset and Configuration Management
SLO Title	**Asset Tracking Database Update Timeliness**
SLO Description	Time to update the asset tracking database with current information after receiving, installing, refreshing or moving Configuration Items.
Time Applicability	Core Hours
Exceptions and Exclusions	Standard Exceptions
Performance Target	≤ 4 business hours after the Configuration Item change is made
Measurement Window	Monthly
Measurement Method	Elapsed Time to reflect all asset changes to the Asset Tracking Database
Data Sources	Help Desk Management System; Asset Tracking Database
Calculation Formula	Total Time for Asset Tracking Database update / Number of Changes
Additional Requirements	
Related PWS section(s)	Sec. 5.6.1.4 Inventory / Asset Management Sec. 5.6.2.3 Change Management Sec. 5.6.3.39 Desk side Technology Refreshment Sec. 5.6.1.3 Integrated Configuration Management (CM) and Asset Management Sec. 5.6.3.43 Inventory / Asset Management Updates

SLO Number	5.3
SLO Category	Asset and Configuration Management
SLO Title	**Software Update / Upgrade Timeliness**
SLO Description	Time to install all commercially released updates, upgrades and patches upon Government approval. For example, upgrades for packages such as Adobe Acrobat, Microsoft Project.
Time Applicability	Core Hours
Exceptions and Exclusions	Standard Exceptions: Non-IAVM related.
Performance Target	Meet all Government directed installation dates
Measurement Window	Monthly
Measurement Method	Actual vs. Scheduled Date
Data Sources	Government written notification from an authorized official; Configuration Management Tracking Tool
Calculation Formula	"Pass" or "Fail" based on missing the target for any scheduled date during reporting period
Additional Requirements	
Related PWS section(s)	Sec. 5.6.2.3 Change Management Sec. 5.6.3 Operational Services Sec. 5.6.3.19 Software Distribution and Upgrades

User Satisfaction

SLO Number	6.1
SLO Category	User Satisfaction
SLO Title	**User Satisfaction Survey Results**
SLO Description	User Satisfaction Survey as administered and tabulated by the Government or a Government-designated third- party.
Time Applicability	n/a
Exceptions and Exclusions	Standard Exceptions
Performance Target	≥ 4.0 on a five-point scale
Measurement Window	Quarterly
Measurement Method	Overall Performance score based on a five-point scale: (1) Poor (2) Fair (3) Good (4) Very Good (5) Excellent
Data Sources	Raw Survey Data
Calculation Formula	Sum of Overall Performance score from each Participant / Total Number of Participants responding
Additional Requirements	
Related PWS section(s)	Sec. 5.6.1.11 Service Level Management Sec. 5.6.3.40 User Outreach

SLO Number	6.2
SLO Category	User Satisfaction
SLO Title	**Operational Level Agreement Compliance**
SLO Description	The contractor's ability to perform against Operational Level Agreements (OLAs) in-place between ITD and other DARPA Organizations
Time Applicability	n/a
Exceptions and Exclusions	Standard Exceptions
Performance Target	"Satisfactory" evaluation from all DARPA Government Organizations with OLAs in-place
Measurement Window	Monthly
Measurement Method	Government POC feedback
Data Sources	POC correspondence
Calculation Formula	Sum of Overall Performance score from each Participant / Total Number of Participants responding
Additional Requirements	*The contractor shall prepare a project plan with Government input and approval to resolve identified User dissatisfaction with contractor performance against Operational Level Agreements.*
Related PWS section(s)	Sec. 5.6.1.10 Operational Level Agreements Sec. 5.6.1.11 Service Level Management

SLO Number	6.3
SLO Category	User Satisfaction
SLO Title	**First Contact Resolution Percentage**
SLO Description	The percentage of **Service Requests** that can be resolved without escalating from Tier 1 support, or re- contacting the User (i.e., Help Desk callback), or a repeat request from the User. Includes Service Requests that can be resolved on the first call (e.g., how-to questions, password/access issues, connectivity related to network settings, software configuration problems, user addressable hardware problems, and other examples as approved by the COR).
Time Applicability	24x7
Exceptions and Exclusions	Standard Exceptions; If desk side support is desired by the User, then the request will not count against the First Contact Resolution metric. Also, does not include requests that require steps outside of the Help Desk or requests that require escalation to Tier 2/3 support by the nature or the complexity of the problem.
Performance Targets	≥ 85%
Measurement Window	Monthly
Measurement Method	Number of Total Requests; Requests Closed at Tier 1
Data Sources	Help Desk Management System (raw ticket data)
Calculation Formula	Requests Closed at Tier 1 / Total Requests * 100
Additional Requirements	
Related PWS section(s)	Sec. 5.6.3.28 Help Desk Services

Professional Services Performance

SLO Number	7.1
SLO Category	Professional Services Performance
SLO Title	**Professional Services Projects Completed On-Time**
SLO Description	Professional service projects were all completed on-time, based on Project Plan vs. Actual variance.
Time Applicability	n/a
Exceptions and Exclusions	Standard Exceptions. Schedule changes outside of the control of the contractor (e.g. requirements additions or significant modifications, lack of availability of the customer for demos or testing, etc.)
Performance Target	All Projects completed on-time during the reporting period (“Pass”)
Measurement Window	Monthly
Measurement Method	Variance between approved schedule and actual delivery.
Data Sources	Project Plan; Actual Completion Date
Calculation Formula	”Pass” or “Fail” depending if completed on-time or not
Additional Requirements	
Related PWS section(s)	Sec. 4.4 Professional Services Projects Sec. 5.6.4.2 Professional Services Projects

SLO Number	7.2
SLO Category	Professional Services Performance
SLO Title	**Professional Services Projects Completed Within Budget**
SLO Description	Professional service projects were all completed within cost budget, based on Project Plan vs. Actual variance.
Time Applicability	n/a
Exceptions and Exclusions	Standard Exceptions; Schedule changes outside of the control of the contractor (e.g. requirements additions or significant modifications, lack of availability of the customer for demos or testing, etc.)
Performance Target	All Projects completed within budget during the reporting period (“Pass”)
Measurement Window	Monthly
Measurement Method	Variance between approved budget and actual cost.
Data Sources	Project Total Cost Estimate/Budget; Actual Total Project Costs
Calculation Formula	”Pass” or “Fail” depending if completed within budget or not
Additional Requirements	
Related PWS section(s)	Sec. 4.4 Professional Services Projects Sec. 5.6.4.2 Professional Services Projects

Program Management Performance

SLO Number	8.1
SLO Category	Program Management Performance
SLO Title	**Reporting Timeliness and Accuracy**
SLO Description	Timeliness and accuracy of scheduled contractor reports and deliverables in the designated format, and according to the specified schedule (weekly, monthly, quarterly, etc.).
Time Applicability	Core Hours
Exceptions and Exclusions	Standard Exceptions
Performance Target	100% accurate and on-time delivery of completed reports and deliverables per reporting requirements
Measurement Window	Monthly assessment, however reporting occurs on a defined time schedule (weekly, monthly, quarterly, etc.)
Measurement Method	Government validation of contractor's report delivery and accuracy of contents
Data Sources	See PWS for specified reports and schedules
Calculation Formula	Number of Reports delivered on schedule and accurately / Total number of reports specified
Additional Requirements	
Related PWS section(s)	Sec. 5.6.1 Program Management Sec. 5.6.1.12 Service Improvement Sec. 5.6.1.11 Service Level Management (SLM)

SLO Number	8.2
SLO Category	Program Management Performance
SLO Title	**contractor Availability, Responsiveness, and Situational Awareness**
SLO Description	The Program Manager or senior-level designee shall be on-site during business hours (7:00 a.m. to 7:00 p.m.). The Program Manager or designee shall be accessible, in person or by phone, for consultation with personnel as identified by the Government. The expectation is within five (5) minutes during business hours and within one (1) hour after Core Hours. Additionally, the Program Management Team shall provide a substantive follow-up to the Government within 30 minutes of acknowledging a performance concern and an update every subsequent 30 minutes during core hours until the concern is obviated—unless otherwise directed. After core hours, the time between updates will be as agreed upon with the Government.
Time Applicability	24x7, with expectations described above.
Exceptions and Exclusions	Standard Exceptions
Performance Target	“Pass” or “Fail”
Measurement Window	Monthly
Measurement Method	Government satisfaction
Data Sources	Government identified personnel
Calculation Formula	“Pass”, “Fail”
Additional Requirements	
Related PWS section(s)	Sec. 5.6.1 Program Management Sec. 5.6.1.13 Service Integration Management

SLO Number	8.3
SLO Category	Program Management Performance
SLO Title	**Upgrades Currency and Maintenance**
SLO Description	The contractor provided service to distribute new and upgraded software to DARPA service delivery points and appropriate DARPA infrastructure. This capability includes, but is not limited to, commercially available off-the-shelf (COTS) software, Government-off-the-Shelf (GOTS), custom application software, end-user and systems services, enterprise functional servers and software licenses.
Time Applicability	24x7 with expectations described above
Exceptions and Exclusions	Standard Exceptions
Performance Target	≥ 99%
Measurement Window	Quarterly
Measurement Method	Vendor shall provide monthly list of software releases greater than N-1. Data logs shall be maintained for Government or designated third-party audit. 99 percent of installed releases are equal to or better than N-1.
Data Sources	Government identified personnel and software vendor publicly available release notes.
Calculation Formula	The number of installed software releases that are equal to or more current than N-1 divided by the total number of software releases, where N is defined as the latest software release.
Additional Requirements	
Related PWS section(s)	Sec. 5.6.1 Program Management Sec. 5.6.1.13 Service Integration Management Sec. 5.6.1.4 Inventory / Asset Management Sec 5.6.1.2 Service Asset (5.6.1.2) Sec. 5.6.2.2 Research, Analysis and Feasibility

4.3.4 Incident Severity Level Definitions

Severity Levels identify the business impact of a network incident/outage.

Level	Definition
Severity 1	Critical functionality loss with widespread impact: • Any issues that affect more than 20 Users simultaneously • Total loss of service or system/service totally stopped Use of system/service is impacted so heavily that work cannot continue • Loss of Security Monitoring Devices impairing Situational Awareness
Severity 2	Minor functionality loss with limited impact: Appropriate as the default or standard severity for outages that affect a system/service Error effects the system/service and causes inconvenience, but the system/service can continue in restricted fashion • Any issues that affect less than 20 Users simultaneously Work-around exists and does not impede Users in their ability to perform their work • Use of system/service is hampered • Minor loss of service When the error affects the service and causes inconvenience, but the services can continue
Severity 3	No immediate impact to application or service functions: • Incident is not important to Users • Incident is not time sensitive for Users • Only non-production environments are impacted

4.4. Professional Services Work Categories

Professional Services projects will be assigned by the COR and managed by the contractor. A description of each Professional Services Category follows with a list of technologies and services of interest to the Government within the Category. Once a first-time project is completed, documentation, transition of knowledge, and training shall be conveyed to support services. Ongoing monitoring and maintenance shall be covered by the support services. The project deliverable shall be added to the Service Catalog. Should ongoing specialized skills be required to maintain the system, the Project Manager shall obtain approval from the Government prior to staff augmentation.

Category 1: Advanced Windows System Integration and Servers Application Support

Advanced Windows Systems support includes the pre-installation planning activities, installation, and problem determination, resolution, documentation, and transition of knowledge of new applications or services. This category shall also include technology trials, pilots, prototypes and proofs of concept, residing on Windows based operating systems that have not been previously

used in the DARPA enclave. These applications and services may require subject matter expertise through product vendors such as Microsoft, to provide state-of-the-art support and implementation of the next generation of services. Examples would be:

a. General COTS/GOTS applications
b. Exchange 2010
c. Network Security Design and Implementation (e.g., Internet Security Appliance (ISA))
d. Domain migration and configuration (e.g., Active Directory)

Category 2: Advanced Non-Windows Systems Integration, Applications and Servers Support

Non-Windows Systems support includes pre-installation planning activities, installation, and problem determination, resolution, documentation, and transition of knowledge of new applications or services. This category shall also include technology trials, pilots, prototypes and proofs of concept, residing on non- windows based operating systems that have not been previously used in the DARPA enclave. Technologies and services included, but not limited to, for this category are:

a. Virtualization platforms
b. Network Appliances (e.g., BlueCoat)
c. UNIX flavors such as Solaris, Linux, HP-UX, etc.
d. Non-Windows based Web Servers

Category 3: Application Analysis, Design and Programming Support

Analysis and programming for systems applications development shall include requirements analysis, detailed specifications, programming and deployment of computer applications whether web-based or distributed (client-server). Application development includes the complete System Development Life-Cycle (SDLC) involved in producing a computer application in addition to following the standard release and deployment process. Examples of systems application development expertise are as follows:

a. Logical and physical database design
b. Web application programming
c. Web application user interface programming (thin or thick clients)
d. Client-server application analysis and programming
e. Object-oriented language analysis and programming
f. SQL programming (SQL or Oracle)
g. Visual Basic .Net Programming
h. Publishing technologies (e.g., PHP and Drupal)

Category 4: Emerging Technologies Research Support

The Government may require assistance in researching and evaluating future and emerging technologies for supporting its mission. The contractor shall provide appropriate subject matter expertise to evaluate the emerging technologies. The primary deliverable of this type of project will be a whitepaper or analysis research papers on the requested technologies, to include a

cost/benefit analysis of available technologies and whether they meet the Government's requirements.

Category 5: Testing and Implementation of IT Research & Development (R&D) Emerging Technologies

The Government may require the testing of IT-related R&D software developed by DARPA technical offices for potential operational use. The contractor shall provide appropriate subject matter expertise in coordinating with the DARPA technical office R&D contractors to create an internal test area for software, establish a secure pilot environment, assist in testing software against DARPA network and workstation standard configurations, and publish results of the testing. If the pilot is successful, upon Government direction, the contractor shall prepare and execute an implementation plan to include the software in the DARPA operational environment.

Category 6: Surge Support

The contractor shall draft for Government approval a Surge Support Plan and may, in order to meet Government-mandated deadlines or in response to a Government request, propose a surge support solution. A costed surge support proposal in accordance with the Surge Support Plan must be approved by the Government prior to project initiation.

4.5 Audio Visual and VTC (AV/VTC)

The AV/VTC Configuration Item shall be comprised of the hardware, software, infrastructure, security features, and services to enable high-bandwidth AV and multi-point IP/ISDN VTC capabilities in, but not limited to, the DARPA Conference Center, lobby display area, small conference rooms, medium conference rooms, large conference rooms, training rooms, and other multi-purpose meeting rooms and areas throughout the building. Based on room profiles, these in-room and infrastructure components include, but are not limited to, room scheduling systems, AV control systems, AV matrix switches, VTC codecs, VTC bridges, multi-domain network video network switches, video displays, video cameras, microphones, power amplifiers, power sequencers, media converters, USB extenders, DVR systems, webcasting systems, guest system AV connections, and classification signs.

Rooms that have been identified to be VTC capable must support both IP and ISDN communications between one or multiple VTC endpoints within DARPA and outside of DARPA, via either DARPA WAN connections to the Internet, NIPRNet, or the Public Switched Telephone Network (PSTN).

Support and maintenance for these systems should include integration with the help desk, configuration management, testing, software distribution and upgrades, user training, remote diagnostics, and support contracts for all AV/VTC COTS components, to include maintenance of the control system software code and multi-domain network video network switch software code that is specific to DARPA**.**

The Audio-Visual Technician (AVT) shall be responsible for installation, maintenance, and support for all AV equipment deployed and supported by the task order. The AVT shall act as liaison between AV vendors and the Government.

5 PERFORMANCE REQUIREMENTS:

This PWS consists of the following functional areas:

5.6.1 Program Management
5.6.2 Infrastructure Services
5.6.3 Operations Services
5.6.4 Professional Services
5.6.5 Analysis and Requirements Services
5.6.6 Software Development, Maintenance, and SharePoint Services
5.6.7 Information Assurance and Network Defense Services

Additional supporting sections are:

5.7 Task Order Transition Services
5.8 Deliverables

Work identified in this document shall meet the levels of service specified in the Service Level Objectives (SLOs). Services in this task order are 24 x 7, however the predominant amount of service tickets are generated during DARPA's core hours between 7am and 7pm, Monday through Friday to a workforce of approximately 1300 personnel.

5.1 General Requirements

The following list of requirements is imperative to the successful execution of the IT services task order. The contractor shall, over the life of the task order increase the maturity of the services delivered to provide cost reductions while at the same time increasing Government satisfaction and productivity.

5.2 Cost-Effectiveness

The contractor shall continuously evaluate the market place to leverage state-of-the-shelf technology. The contractor shall make every effort to implement cost-effective services and solutions. DARPA also acknowledges that the most expensive up-front cost might have the highest return on investment (ROI) and therefore be the best choice. When appropriate, the contractor shall present DARPA with evaluations of potential solutions that demonstrate immediate savings versus long-term savings; savings must be demonstrated over the anticipated life-cycle of the possible solution.

5.3 Access and Ownership

All DARPA information resources and contractor generated data such as system log data, documentation, program code, automated scripts and ancillary information under the task order is owned by the Government. As such, the contractor must allow and provide capabilities for authorized Government managers and staff, as well as designated contractors, access to such data. Deliverables shall be made available in a shared repository available at all times to the Government; currently SharePoint services are being used for this purpose. Upon request by the Government, the contractor shall, without delay, deliver and convey any/all requested DARPA files/documents, etc. to the appropriate DARPA person or organization. Likewise, the contractor must provide on-going direct systems/automated access to DARPA files and databases. Such direct systems access shall include administrative or root type access for the purpose of oversight, generating reports, forensics and analysis. Management consoles must be accessible for

validation/monitoring purposes. Deliverables required by the task order are Government property and may be redistributed within the Agency for management or verification purposes. Additionally, the Government reserves the right to reach down to contractor personnel directly while simultaneously coordinating with contractor Management in order to support urgent requirements or emergencies.

5.4 Unified Communications

DARPA requires the integration of communication services to provide a consistent unified user-interface and user-experience across multiple devices and media types.

5.5 Personnel Standards

The contractor shall provide mid- to expert-level staff with the necessary skills appropriate for the various job types on this task order in accordance with Attachment 8. The Government requires certified and experienced staff so that the quality of service is exemplary and the response times to incidents, requests, and problems are minimized. The contractor shall maintain qualified personnel in compliance with DoD Directive 8570.01 (Reference (g)).

5.6 Functional Area Tasks

There are seven primary Functional Areas Tasks detailed below:

a. Program Management
b. Infrastructure Services
c. Operations Services
d. Professional Services
e. Analysis and Requirements Services
f. Software Development, Maintenance, and SharePoint Services
g. Information Assurance and Network Defense Services

These Areas are intended to cover the entire life-cycle of support for DARPA's information technology service, support, and infrastructure environment.

5.6.1 Program Management

The contractor shall provide effective, efficient, and responsive program and project management, financial management, and task order administration services for this PWS. The management team shall be exclusively dedicated to this task order. SLO 8.2 applies. The contractor shall provide a management team that is responsible for interfacing and collaborating with the Government and other contractors' management, formulating and enforcing work and quality standards, establishing schedules, reviewing work in progress, developing standard operating procedures (SOPs) and managing personnel. DARPA requires the contractor to assist in strategic planning to include the drafting of business and technology strategies, technical architecture to support the strategies, and conducting the research of new technology trends, products and services, such as hardware components, system software, and networks that offer opportunities to improve the efficiency and effectiveness of IT services.

The Program Manager (PM) shall be responsible for the overall management of tasks performed under this task order and shall be the primary point-of-contact for task order issues. The PM shall be responsible for ensuring that practical and effective systems are developed to meet the task order requirements. The PM shall also be responsible for ensuring the quality and

timeliness of the work performed and for process improvements that result in cost effectiveness and savings for the Government. The PM and Deputy Program Manager (DPM) shall function as a cohesive team responsible for financial, contractual, project management, technical and security actions on behalf of the contractor.

The Deputy Program Manager (DPM) shall be responsible for sharing the duties of the contractor's PM and empowered to take action as a designee when the PM is unavailable. The DPM shall manage network and security projects, act as the liaison between contractor staff and the PM, and serve as the lead technical POC for the contractor to communicate issues and concerns in a comprehensive and timely manner to the Government.

The Service Operations Manager (SOM) shall oversee the operational services personnel who manage the servers and network services. The SOM reports on Network availability and server up-time per SLO and PWS requirements.

5.6.1.1 Service Asset & Configuration Management
With advance Government approval, the contractor shall be responsible for purchasing, inventorying, and decommissioning Configuration Items (CIs) in accordance with NSA/CSS Information Assurance Directorate CGS (Reference (l)). These activities include, but are not limited to:

a. Technology Insertion
b. Technology Refreshment
c. Technology Enhancement
d. Capacity Planning

5.6.1.2 Service Asset
The contractor shall provide and support DARPA Service Assets to achieve optimal performance and user satisfaction. The contractor shall provide support services with security features for the general DARPA enterprise infrastructure and external networks to produce an effective and efficient interface with commercial, DoD, and Government communications environments. All service asset configurations (hardware and software) shall be proposed by the contractor and submitted in advance of deployment to the Configuration Control Board (CCB) for approval as outlined in the DARPA IT Configuration Control Governance Process. Procurement of service assets shall be initiated by User orders via the DARPA Store Front. Refer to DARPA Store Front definition for additional information. As they are considered service assets, the contractor shall obtain and manage software licenses in accordance with DISA Application Security and Development STIG (Reference (k)). The contractor shall monitor and audit all software licenses to preclude inadvertent license and maintenance expiration (see SLO 8.3). Additionally, the contractor shall track all follow-on costs associated with software (licensing, maintenance, etc.) reporting quarterly and in coordination with the ITD Budget cycle. The Government reserves the right to purchase and own bulk licenses. All procurements shall be in accordance with the Clinger-Cohen Act of 1996 (Reference (p)). If authorized by the Contracting Officer in accordance with FAR 51.102, the contractor will be allowed to use GSA Schedule Contracts, or other Government procurement vehicles (i.e., the DoD Approved Software, Enterprise Software Initiative (Reference (o)) with the goal of decreasing cost.

5.6.1.3 Integrated Configuration Management (CM) and Asset Management Control Process

The contractor shall develop and implement within 90 days of task order award, a centralized configuration management control process encompassing the complete inventory of hardware, software, documentation, and processes maintained in a Configuration Management Database (CMDB). The CMDB shall contain all CIs and provide the capability to map relationships of CIs to other CIs, including systems, devices, applications, groups, and individuals. The Service Catalog shall be a part of the CMDB. The CMDB shall also house the "as built" system documentation including configurations of legacy systems (including network diagrams), which will be used for certification and accreditation (C&A) activities. The contractor shall develop, maintain and keep current the CMDB.

The contractor shall provide and maintain a software library to include authorized and deployed software configurations. The contractor shall provide a Cable Management plan of all cables within the DARPA enclave, wiring closets, and conference rooms. The contractor shall assist the Government in implementing an enterprise-wide change management process to encompass all changes to the supported unclassified network infrastructure. The contractor shall present to, and provide technical and administrative support for the CCB. The contractor shall present all proposed technology refreshment, technology insertion, or technology enhancement changes for each section of this PWS to the CCB. The contractor shall document the benefits to be achieved for DARPA in terms of effectiveness and efficiency in an impact assessment of proposed technology changes on Agency cost. The CCB must authorize all proposed technology refreshment changes.

5.6.1.4 Inventory / Asset Management

The contractor shall maintain a complete and current asset inventory in the Government-owned database of all hardware, software and software licenses, maintenance/subscription agreements, and maintain a logical relationship record of the items in the asset inventory. The Government is currently using Remedy for this purpose. The accuracy of the Inventory shall be in accordance with the Inventory Reform Act of 1998 (Reference (q)) and SLO 5.1. Changes to the assets inventory shall be reflected in the configuration management system in accordance with SLO 5.2. The contractor shall procure, inventory, track, and manage software and licenses for all in-scope commercial software applications on a continuous basis with updated inventory by User and device no more than one business day after deployment. A "Software Asset Inventory and License Report" shall be produced on the first of each month customized for each DARPA Office and made available to the Government. In addition, the contractor shall make the database containing that information available to the Government in near real-time. The contractor shall track patches, upgrades, and expiration dates for all software deployed on user systems, and notify the Government and the user when changes occur. No cost upgrades and patches shall be performed without Government approval. Upgrades shall be in accordance with SLO 8.3. The asset inventory database shall be accessible by the Government, and shall include at a minimum the ability to query by bar code, CLIN, assignment date, User name, directory/office assignment, and cost. The contractor shall implement processes to audit and control inventory, to ensure that all unclassified IT assets, (software, devices, and peripherals) are accounted for. The contractor shall ensure at least annually that each unclassified IT asset is verified visually. The Government may designate personnel to accompany contractor personnel to validate audits. The Asset and Credit Report must be accessible to the Government electronically in near real-time.

5.6.1.5 Demand Management

At a Strategic level the contractor shall analyze the patterns of business activity and user activity. The contractor shall anticipate and address Government and user requirements for new and or enhanced services to include software, hardware, support, and infrastructure services. The contractor shall inform and recommend cost-effective options and processes, and their implications, to satisfy IT service requirements.

5.6.1.6 Service Portfolio Management

The contractor shall manage a portfolio of services from the inception of a service through deployment of the service to retirement. The contractor shall provide information to the Government detailing the life-cycle of each service or configuration item and the impact the service transition has upon the DARPA IT environment.

5.6.1.7 Service Management

The contractor shall establish and maintain the Service Pipeline, listing all IT services that are under consideration or development, but are not yet available to the Government. The contractor shall establish and maintain the Service Catalog which shall contain information about all available IT Services, including those available for deployment. The Service Catalog shall be used to support the charge and delivery of IT Services to the Government. The Service Catalog includes information about deliverables, prices, contact points, ordering, and request processes. As part of the tracking of the service lifecycle, the contractor shall maintain a list of all services removed from the Service Catalog (retired) in the Service Portfolio.

5.6.1.8 Service Database / Repository

The contractor shall establish and maintain a service database to contain the Service Portfolio. The database and the data held therein shall be the property of the Government.

5.6.1.9 Service Catalog Planning

The contractor shall work with the Government to ensure the proper planning and coordination is in place for the transition of Configuration Items from the Service Portfolio to the Service Catalog.

5.6.1.10 Operational Level Agreements (OLA)

The contractor shall support existing Operational Level Agreements.

5.6.1.11 Service Level Management (SLM)

The contractor shall ensure that all IT Service Management Processes, Operational Level Agreements, and Underpinning Contracts, support the Service Level Objectives. The contractor shall monitor and report on Service Levels, and hold regular Government reviews. Reporting of the task order SLOs and deliverables shall be accurate and timely in accordance with SLO 8.1.

5.6.1.12 Service Improvement

The contractor shall develop a methodology for managing continual service improvement with particular attention given to cost savings and operational efficiencies through the use of Service Delivery Maturity models. The contractor shall provide flexible and innovative solutions to the Government.

The contractor will ensure that the following requirements are met:

a. Develop and receive approval for a Service Delivery Maturity Plan
b. Participate in a joint working group with the Government that will continually measure and report on the progress of achieving service delivery maturity
c. Develop a SDLC process and documentation to be compliant with applicable service maturity model(s) for Government approval

5.6.1.13 Service Integration Management

The primary goal of IT governance is to identify, control, and track the introduction of Configuration Items and changes to the IT environment. The role of the Government is to provide leadership and oversight. The contractor's role will be to perform all activities necessary to allow for the integration of information technology within DARPA enclave. The contractor shall perform the following:

a. Infrastructure Architecture – this includes all hardware and network services
b. Software Architecture – this includes all software authorized and Government or contractor owned
c. Security Architecture – this includes all software and hardware required to provide DARPA's network with the necessary tools to ensure proper IT security
d. Service Architecture – this includes service support, operations, and professional services

5.6.1.14 Management and Administration

The contractor's Program Manager or designee shall support IT governance in the following ways:

a. Attend Government directed morning stand-ups
b. Ensure the status and progress of each item of work being performed on a near-real time and monthly basis and the monthly Financial Report are submitted
c. Hold in-process reviews on a quarterly basis with the Government. Issues to be addressed include:
    i. Strategic planning
    ii. contractor performance with respect to quality, schedule, cost, and cost savings
    iii. Summary review of detailed Plan of Action and Milestones (POA&M) for each initiative
    iv. Metrics that portray the progress of work under the task order
    v. A summary of the quality of work performed from the points of view of DARPA Users such as via surveys, and
    vi. Plans for improvement of the contractor staff to achieve more effective and efficient support of the DARPA mission

5.6.1.15 Program Coordination Support

The contractor shall provide technical and managerial support and input to Government program boards, panels, reviews, teams, working groups, and various ad-hoc meetings and committees. Some meetings require the contractor to give formal briefings, while others may only require attendance and participation. The contractor shall support these meetings and reviews with the level of technical and managerial participation sufficient to meet the needs of the meeting or

review. Examples include, but are not limited to:

a. Configuration Control Board (CCB)
b. Configuration Control Board Working Group (CCBWG)
c. Ad-hoc Committees/Boards
d. Outage Reviews
e. Management and Task Order Reviews
f. Monthly Technical Operations Reviews
g. CO/COR Meetings

As directed by the Government, the contractor shall take and submit meeting minutes for Government approval no more than one working day from the end of the meeting.

5.6.1.16 Ad Hoc Services
The contractor shall provide support for ad hoc services, within the general scope of this requirement, as requested.

5.6.2 Infrastructure Services
The Infrastructure Services functional area is responsible for providing network connectivity as well as the essential base network services and resources. These include, but are not limited to LAN services, Intranet and Extranet services. The contractor shall provide all support for the network infrastructure and the network servers. The contractor shall coordinate with the Government to ensure power, space and cooling requirements and concerns are met. The maximum scheduled downtime for all network services shall comply with SLO 2.9.

Infrastructure Services shall be in accordance with DoD Directive 8320.02 (Reference (a)) and comply with SLO 2.4. Infrastructure services build on the base network connectivity and focus on the essential network services; these services include, but are not limited to:

a. IP address management
b. Machine Address Code (MAC) management
c. Directory Services management
d. DHCP Management
e. DNS Management
f. Unified Communications

The Infrastructure Manager/Network Architect (IM/NA) shall be responsible for maintaining the required service level objectives for the network through network monitoring as well as technology enhancement, capacity planning and future implementations of new network technologies. The IM/NA position includes responsibility for capacity planning for increased demands of video streaming (multicast) and other technology advances. The Infrastructure Manager will oversee the overall network functions and at times may be required to act as a Network Engineer.

5.6.2.1 Transition Planning & Support
The contractor shall provide transition planning and support for all new services to be transitioned from development into production. Transition Planning and Support shall include the following processes:

a. Release and Deployment Management
b. Service Validation and Testing
c. Integration and Testing

5.6.2.2 Research, Analysis and Feasibility
The contractor shall assess the feasibility and utility of emerging technology based upon Government direction. The contractor shall conduct the technical research, reviews, pilots and trials as needed to evaluate new technologies. Once a technology is approved, the Government will present the contractor with a Project Request, where the contractor will provide a project plan based on the Government's requirements, detailing the time, cost and proposed personnel to complete the work. Plans should be in a Government approved format suitable for providing to user for review/approval. The contractor shall provide flexible and innovative solutions to the Government as detailed in SLO 8.3.

5.6.2.3 Change Management
The Configuration Control Board (CCB) reviews updates and changes to the current infrastructure, to include network resources, technology refreshment, technology insertion, or technology enhancement changes, on the schedule provided by the Government or on an ad-hoc basis due to unexpected capacity changes and growth, usually limited to servers and networking equipment.

The contractor shall participate in the change management process (CCB) as specified by the task order Program Management office and Government oversight to facilitate proper registration of all Systems Engineering and Planning projects that result in configuration changes.

5.6.2.4 Support to the Configuration Control Board (CCB)
All configuration changes shall go through the Government-controlled CCB change process (see Attachment 6). The contractor shall participate in and provide technical support for the CCB. In support of the CCB, the contractor shall track the status of all changes to any Configuration Item and update the Configuration Management Database (CMDB). Ad hoc recommendations proposed by the contractor shall be made as needed in conjunction with Government oversight. The contractor shall not make changes to the Government's IT architecture without authorization from the CCB. In the event of an emergency, CCB emergency procedures shall be followed.

5.6.2.5 Release & Deployment Management
The contractor shall provide all documentation (SOPs, FAQs, etc.) to support the Release and Deployment processes. Releases and deployments shall be planned, tested, scheduled and implemented to avoid any unscheduled downtime or impact to the production environment.

5.6.2.6 Technology Refreshment, Insertion and Enhancement
The contractor shall provide capabilities to support the technological evolution and planning of changes to all components in the DARPA unclassified networks. Specifically, the contractor shall estimate future requirements (including capabilities, volume, usage, and application characteristics) as well, as integration of emerging technology, to meet evolving DARPA requirements. The contractor shall conduct a bi-annual analysis of the enterprise (all network components and Government-owned/Legacy assets), and present to the Government recommendations for end of life, expired or changes necessary to maintain security compliance or contractual, operational requirements. The contractor shall procure licensing and warranties for

all hardware, as well as, software maintenance for all software based on the refreshment/replacement cycles listed below. The contractor shall make every effort to ensure minimal impact to users during refreshment, insertion and enhancement activities. The contractor shall ensure the accuracy of any data transfers and carryovers from the existing to the new technologies. The contractor may use surge support according to the Surge Support Plan and with Government approval. The following technical refresh schedule is envisioned:

a. Mobile Devices: 24 months
b. Tablets: 24 months
c. Laptops: 24 months
d. Desktops: 24 months
e. Conference Room electronic equipment, as agreed to by the Government: 24 months
f. Printer/Copier Devices: 48 months
g. Software (included in the basic image): N-1

The contractor shall plan for and execute all technology refreshment projects such that the completion date is no more than the specified number of months from the previous refreshment. Equipment that is refreshed will be disposed of in a manner consistent with DoD and DARPA policies. Hard drives and other components that retain data will not leave DARPA control until the data is cleared or destroyed using processes approved by the DARPA Authorizing Official (AO) (Reference (x)).

5.6.2.7 Service Validation and Testing

For every new service, or major modification to an existing service or application, the contractor shall, in coordination with the Government, incorporate in the development, release and delivery processes, stages that test the validation of the service. Validation and testing ensures that the IT infrastructure, including power, rack space and servers can support the new service and meet user expectations.

The contractor shall have a service validation and testing process to ensure that release and deployments of applications and services do not affect performance of the associated systems and the resulting services meet user expectations.

The contractor must ensure that the IT operations team will be able to support the new applications and services. Results of the testing will be provided as part of the package sent to CCB for approval.

5.6.2.8 Integration and Testing

The contractor shall conduct pilots and testing of new software, patches, security patches and security updates, as well as new hardware. The contractor shall conduct system-level testing of all software to validate that it performs in accordance with approved specifications and can be deployed successfully and operate with supported software images on approved hardware.

The contractor shall have integration and testing processes as part of each Professional Services project (defined in Paragraph 5.6.4). Testing will verify functional, performance and reliability requirements of all new applications and systems to be introduced into the DARPA enclave. Results of the testing will be provided as part of the package sent to CCB for approval.

5.6.2.9 Interoperability Test Plan
The contractor shall have and maintain an Interoperability Test Plan for ensuring that new applications and services introduced to the DARPA enclave will integrate and interoperate with existing applications and services.

5.6.2.10 Knowledge Database(s) Maintenance
The contractor shall provide process improvement by implementing methodologies to capture IT knowledge resulting in improved service and support over the life of the task order.

5.6.2.11 On-Line Collaboration Site Development and Maintenance The contractor shall provide application analysis, design and programming services for the creation and maintenance of on-line collaboration and websites. These services shall be included in the Service Catalog. The Government currently uses Microsoft SharePoint Designer 2010.

5.6.2.12 Directory Services (DS)
The contractor shall provide and maintain centralized directory services for all networked users and resources that supports the management and utilization of file services, network resources, security services, messaging, web, e-business, white pages and object based services across DARPA. The Windows Active Directory service is currently in use. The Infrastructure Services team shall work collaboratively with the Support Services and Operations teams to provide seamless support for Access Management.

The contractor shall provide the following via Directory Services:

a. Compliance with DoD Enterprise Directory Services Capability Document
b. Support for PKI authentication services, currently DoD Common Access Card (CAC). The capability shall be provided for users, devices and applications to discover and utilize global information services data. Office numbers, telephone numbers, DARPA-issued wireless and fax numbers, and e-mail addresses shall be maintained and available to all DARPA personnel
c. Support the monitoring of administration and management network resources
d. Support the current implementation of global account management and subsequent authentications and authorizations to data maintained in the global directory services team
e. Support the enablement of and distribution of applications
f. Provide a proactive environment that builds and manages relationships between objects within the global directory service

5.6.2.13 IP Address Management
The contractor shall provide IP address management for the DMSS and DPN.org networks. This will include managing the provisioning of IP ranges for all Service Delivery Points for both networks. IP address support shall be provided for DHCP, IPv4, IPv6, VoIP, Unified Communications, audio and video conferencing as well as fax, print, and copy services.

5.6.2.14 Machine Address Code (MAC) Management
The contractor shall track MAC addresses for all applicable user devices.

5.6.2.15 IP Version 6 Support

The Government has an Autonomous System Number (ASN) and an associated IP version 6 (IPv6) address range assignment for future implementation in accordance with "Memorandum for CIOs of Executive Departments and Agencies, Subject: Transition to IPv6," dated September 28, 2010 (Reference (m)). All information systems equipment purchased for DoD agencies and organizations shall be IPv6 capable and in compliance with DoD IPv6 Standard Profiles for IPv6 Capable Products (Reference (n)).

5.6.2.16 Domain Name Server (DNS)

The contractor shall provide DNS services to the Government networks providing both internal and external name to IP resolution and apply the current STIG. DNS, where applicable, will be integrated with Directory Services to take advantage of DNS features such as secure dynamic updates, record aging, DNS Security Extensions (DNSSEC) and scavenging features. The DNS services shall meet all functionality of the current Domain Name Server (DNS) service, to include flexible support for offsite locations to retain the darpa.mil domain naming convention.

5.6.2.17 Dynamic Host Configuration Protocol (DHCP)

The contractor shall provide DHCP services for auto configuration of IP address and network information for the Government networks. The contractor shall assign DHCP address ranges for both the DMSS and DPN.org networks.

5.6.2.18 Intranet/Extranet Services

The contractor shall provide Intranet and Extranet services to the DARPA enclave and comply with SLO 2.6 for Server Services Availability.

5.6.2.19 External Network Access and Services

The contractor shall provide external network services that are transparent to DARPA users but are essential to Government telecommunication functionality, security, performance, and interoperability. "Network service" refers to the various management and operational activities, hardware, software, connection service, and transmission media necessary for the delivery of internet and telecommunications services to internal and external DARPA users. External Networks shall include connectivity and transport services to, from, and among all Government Service Delivery Points and other non-DARPA organizations. Specifically, to meet the Government requirements for external network access and services, the contractor shall provide redundant Commercial Network Services, which provide connectivity to external network services such as the Internet and telecommunications. The contractor shall provide Internet access in accordance with SLO 2.2 for all Government Service Delivery Points (SDPs) with sufficient bandwidth to meet performance specifications, service levels, and security requirements as stated in the task order. In addition to Internet connectivity for the DMSS network, the contractor shall provide separate Internet connectivity for DPN.org, which exists as a separate network designed specifically to allow DARPA personnel to connect to universities and other institutions with fewer restrictions than on the DMSS. The contractor shall provide monitoring, maintenance and support for network devices, including, but not limited to, routers, switches and firewalls on both the DPN.org and DMSS networks.

The Non-classified Internet Protocol Router Network (NIPRNet) is used to exchange sensitive but unclassified information between "internal" users as well as providing users access to the Internet. The contractor shall support connectivity to the NIPRNet through the DMSS network.

5.6.2.20 Local Area Network (LAN) Communication Services

The contractor shall provide the capability to interconnect geographically co-located and separate DARPA Local Area Networks (LANs) and attached devices. The current DARPA LAN is limited to the Founders Square and Disaster Recovery locations. Connectivity may be extended, at the Government's request, to any required space.

5.6.2.21 Internal (LAN) Connectivity

The contractor shall provide and maintain internal LAN connectivity and security services to networked Service Delivery Points (SDPs). The security services are described in Information Assurance and Network Defense section 5.6.7 of this PWS. The contractor shall comply with SLO 2.1.

5.6.2.22 DARPA Intranet Services

The contractor shall provide and maintain a DARPA intranet that is an unclassified, private, web-based portal that utilizes Active Directory and is specifically designed for DARPA users to conduct internal business. The contractor shall provide a service whereby DARPA users may access services, data and files on the Intranet from remote locations, and search the contents of DARPA intranet web pages. For users located outside a DARPA firewall, the contractor shall provide the capability to access the DARPA Intranet with security features. Virtual Private Network (VPN) solutions may be used, but VPN devices used within DARPA shall be selected and implemented in accordance with configuration management processes.

The contractor shall provide the capability for web-crawling, site indexing, security features, and a search engine. Additional services such as authoring of the web content and application development for DARPA users may be ordered under the contractor catalog services. The contractor shall provide web/Intranet support to DARPA organizations which have created intranet content that extends beyond the scope of DARPA Intranet Services. This support shall include tasks and activities associated with mid-level support and shall consist of tasks that do not require senior developer expertise or engineering support. Examples of these tasks include, but may not be limited to the following:

a. Code reviews
b. Tool usage support and direction
c. Troubleshooting and instruction
d. Basic site management

5.6.2.23 DARPA Extranet Services

The contractor shall provide, maintain, and support a DARPA Extranet secured via PKI, External Certificate Authority (ECA), or password access, as necessary that provides a secure point of entry for DARPA-authorized users to upload, download, and access services, data and files from remote locations, and collaborate with other users, including DARPA personnel.

5.6.2.24 Remote Access

The contractor shall provide services that allow DARPA users 24x7 access to the DARPA intranet and data network from remote locations via a virtual private network (VPN) and comply with SLO 2.3. Access to the intranet via VPN shall require the identification and authentication of the user via DARPA-approved two-factor authentication. The service shall interface with Directory Services to verify user authorization. The contractor shall provide increased Remote Access capacity as directed to accommodate Government network access surge requirements. In

accordance with DoD Instruction 8500.01 (Reference (y)) remote access accounts shall be operated in a way that prevents them from being used to administer the network or conduct administrative functions unless waived by the Government. If remote administration is required, it shall require separate accounts with special privileged access, and additional logging.

5.6.2.25 Capacity Management
The contractor shall monitor the capacities of all network resources and ensure that they are adequate to the Government's needs, meet or exceed industry best practices, and are compliant with the Government-designated thresholds. The contractor shall provide recommendations when performance drops below DARPA-approved thresholds.

5.6.2.26 Throughput / Bandwidth Monitoring
The contractor shall monitor the throughput and bandwidth utilizations of the entire unclassified DARPA enterprise, identifying a day-to-day baseline. From that baseline the contractor shall identify peaks and anomalies in network traffic for capacity planning and for identifying potential network incidents. If the contractor finds that network segments, connections, core switches, and connections to external networks are consistently hitting peaks near or at 70%, the contractor shall bring it to the attention of the COR, identify the root cause, and propose a mitigation or resolution strategy.

5.6.2.27 Storage Capacity Monitoring
The contractor shall monitor the storage capacity for all network servers and services, and shared file storage solutions. The contractor shall notify the COR if file systems exceed Government-specified thresholds.

5.6.2.28 Availability Management
The contractor shall monitor all networked resources to ensure that they are available. The contractor shall address and resolve any issue that reduces the availability of the network according to severity levels and the timeframes specified in SLO 3.2. The contractor shall respond and inform the Government of any network issue in accordance with SLO 3.2.

5.6.2.29 Network Management System (NMS) Service
The contractor shall provide a Network Management System (NMS) to monitor and administer the unclassified networks. The NMS services provided by the contractor shall include fault management and participation in the configuration management process, access management, and performance management. The contractor shall make available to designated Government entities, near real-time information feeds to support Government oversight, maintain accessible historical data, provide summary management reports that detail the NMS functions, and allow the contractor to forecast networking requirements through the use of modeling techniques.

Specifically, the Government requires that the contractor shall provide a centralized network monitoring service that will comprehensively monitor the DARPA unclassified networks on a 24x7-basis. The Government requires that the contractor provide sophisticated capabilities for real-time monitoring of performance and utilization levels for all segments of the contractor-supplied network infrastructure. The scope of monitoring should extend to the edge router at each partner site and include devices and applications through which users connect to the network remotely. The monitoring service shall provide the following capabilities and services:

a. Best practice monitoring of email, Directory Services, File Services, etc.

b. SNMP monitoring of all active network devices serving the Government
c. Operate a 24x7 monitoring facility, properly equipped and staffed to identify and mitigate network faults and failures throughout the entire DARPA enterprise
d. Comprehensive performance monitoring capabilities that extends to each Government edge router
e. Comprehensive performance monitoring capabilities that track availability and performance of network links at DARPA connection and peering points withternal networks
f. Regular periodic reporting to Government and individual DARPA Partners as appropriate, for network performance and reliability according to SLOs 2.1 and 2.2
g. Government-accessible, real-time, Web-based services that provide comprehensive network status information
h. Government-accessible, web-based problem reporting facilities that support ticket generation, ticket status updates and ticket resolution notification
i. Resource utilization reports that document usage

5.6.2.30 Network and Security Operations Center

The contractor shall provide personnel to staff the Network and Security Operations Center (NSOC) which shall operate 24x7. The NSOC shall provide network, server, IA and availability monitoring services (including classified (Secret-level) information and reporting), incident management and perform other tasks as directed by the Government. NSOC core hours are from 7am to 7pm, with a minimum of two people from 7pm to 7am.

The NSOC shall provide the NMS services as specified in section 5.6.2.29. The NSOC shall provide support to the Help Desk as required. NSOC personnel shall follow contractor-issued, Government-approved escalation procedures for specified events and outages, which may include notifying Government personnel and participating in CIRT/CERT response teams. The contractor provided NSOC shall include a Trouble-shooting bridge with a staffed Incident Manager.

5.6.2.31 Security Information and Event Management (SIEM) System

The contractor shall provide a Security Information Management System to act as a central repository for the collection of all security data (e.g., event logs), provide trending, reporting, charts and graphs both in real time and extending to a period of no less than 13 months. The contractor provided SIEM shall conduct real-time monitoring, correlation of events, notifications and console viewing, as well as, long-term storage, analysis and reporting of log data. Additionally the SIEM will be responsible for the monitoring of user and service privileges, directory services, network incident review and response.

5.6.2.32 Network Hardware Services and Maintenance

The contractor shall provide hardware services and maintenance for all DARPA enterprise networks (DMSS and DPN.org). The contractor shall evaluate the hardware upon which the Infrastructure Services are built and recommend to the Government when upgrades, repairs or replacements are necessary. The network hardware shall be compliant with IA and DoD Policies as well as being certified for use within the enclave.

5.6.2.33 Network Technology Refreshment

The contractor shall refresh networking equipment as required. The contractor shall purchase warranties, vendor maintenance, and licensing for all networking equipment and software until refreshment/replacement. A networking equipment technology refresh shall be initiated due to

any one of the following events:

a. Equipment is incapable of supporting new technological requirements (e.g. IPv6 or PKI) as required by the Government or DoD requirements
b. Equipment can no longer support the demand and capacity of the organization
c. Equipment is "End-of-Life" and no longer supported by the Vendor
d. Equipment warranty will soon expire and is not eligible for renewal

All proposed networking equipment technology refreshes must be approved by the CCB.

5.6.3 Operational Services

The contractor shall provide full life-cycle support (i.e., vendor offered warranties, licenses, and maintenance agreements) for all of the services identified in this PWS. The underlying support for services are Server Operating Systems, Server hardware and the associated maintenance, compliance with records management for capturing server and service activities, and technology refreshment of servers and services. The maximum scheduled downtime for all servers and services shall comply with SLO 2.9.

5.6.3.1 Server Operating System Support

The contractor shall provide, as a service, the installation of the Government approved server operating system and maintenance of the operating system by applying hot fixes, updates and services packs. Specifically, the contractor shall provide, at a minimum, the following services for all unclassified servers covered under this task order:

a. The service or application provided by the underlying server(s) shall be maintained with minimum downtime or service degradation and maximum availability in accordance with the Service Availability SLO 2.6
b. Per CND and IA policies and procedures, maintain the current versions of security patches and appropriate security configurations and relevant DISA STIGs for server operating systems and applications unless waived by the Government.
c. Enforce, protect, and change passwords or enable PKI in compliance with Government and IA policies (Reference (y))
d. Track and report on SLOs for specific servers as required (e.g., Email Servers, SLO 2.5)
e. Review, maintain, provide alerts and archive server system events logs as specified by DARPA Security and Intelligence Directorate (SID) or in DoD Directive 5015.02-STD (Reference (b))
f. Respond to all monitoring alerts which may indicate degradation in service, an outage, or hardware failure
g. Troubleshoot and resolve server related hardware and software failures
h. Provide third tier support to include, but not limited to, end-users, Help Desk staff and other functional area staff as needed
i. Provide an automated method (dashboard) for daily operational status updates to keep management, the Help Desk, the Government and the end-users informed about the system issues

5.6.3.2 Server-Side Hardware Services and Maintenance

The contractor shall make server hardware recommendations based on the type of application or service the server will be providing to the Government. The contractor shall create standard

server hardware builds based on Government requirements and CCB approval, as well as, provide custom server builds for high-end and specialized needs. The contractor shall make recommendations for advanced server technologies that will benefit the User and provide the best User experience.

5.6.3.3 Unified Communications (UC) and Telephone Services
The contractor shall support Unified Communications and telephone services, including Voice-over-IP (VoIP), Public Switch Telephone Network (PSTN), Sectera vIPer phones, and Plain Old Telephone Service (POTS). The contractor shall provide the capability, features, and security, to enable users to make and receive phone calls. The contractor shall make training available for unified communication services, including chat client, messaging and equipment. The contractor shall plan and make acquisitions with the knowledge that VoIP is a requirement. The telephone services availability shall comply with SLO 2.7.

5.6.3.4 E-mail Services
E-mail is an integral part of DARPA and shall conform to industry standards for interoperability and remote access and comply with DARPA conventions for domain naming (i.e., retention of DARPA.mil domains) and e-mail account naming conventions (e.g. first.last.ctr@darpa.mil for all contractors). The contractor shall ensure that foreign nationals are clearly identifiable in electronic communications in accordance with DoD Directive 5230.20, Visits and Assignments of Foreign Nationals (Reference (z)). The contractor shall provide all E-mail functionality and services supporting the customer including, but not limited to sending, storing, processing, searching and receiving electronic messages and multimedia e-mail attachments. The Government currently uses Microsoft Exchange 2010. The services shall be configurable to provide the capability for sending and receiving signed and encrypted e-mail and attachments, by utilizing the DoD standard, currently PKI compatible user certificates, and in accordance with DoD Enterprise Directory Services Capability Document (Reference (u)) and in compliance with industry best practices. Each end-user shall be supplied with an e-mail account and desktop client to be supported by Support Services. SLO 2.5 applies.

The Government currently has no storage quotas for user's e-mail.

5.6.3.5 Internal Chat Services
The contractor shall provide internal instant messaging/chat services through DoD and Government approved applications. The Government currently uses Cisco Jabber. The contractor shall provide web content filters, firewall controls and/or other industry standard block procedures as approved by the CCB, which will prohibit or monitor internet chat activities.

5.6.3.6 Social Networking
The contractor shall provide DARPA users social networking capabilities on the Government Intranet for sharing ideas and thoughts that are sensitive and internal to the organization.

5.6.3.7 Fax Services
The contractor shall provide the capability and features, to include security, allowing users to send and receive faxes via e-mail. The Government currently uses Captaris RightFax for e-mail fax services. The contractor shall make e-mail-based fax service training available. The

contractor shall comply with SLO 2.7 for the associated telephone services as well as SLO 2.6 for Server Services Availability.

5.6.3.8 Print Services

The contractor shall provide network connectivity to print services. The contractor shall monitor the printers for user availability. The contractor shall provide an IP addressing scheme that complies with DoD guidance for secure communications (Reference (k)). .

5.6.3.9 Copying Services

The contractor shall provide network connectivity and CAC services to Government-furnished printing and duplicating machines located on each floor of the DARPA enclave to enable high-speed and quantity printing services. The contractor shall provide an IP addressing scheme that complies with DoD guidance (Reference (k)) for secure communications.

5.6.3.10 Compliance with Records Management Policies

The contractor shall be in accordance with DoD Directive 5015.02-STD (Reference (b)) and maintain compliance with records management and retention policies by utilizing a centralized log repository. The contractor shall provide the Government with direct read and direct reporting access to the centralized log repository to allow Computer Network Defense functions, security oversight and records management functions.

5.6.3.11 Access Management

The contractor shall provide Access Management services providing DARPA's users access to networked resources through the use of Directory Services (DS); currently DARPA is using Active Directory for user account management, Group Policies, Group Membership, Access Rights, and Delivery. In compliance with IA and Computer Network Defense (CND) policies (Reference (y)), the contractor shall utilize directory services to provide access to network resources using the Principle of Least Privilege which shall be enforced for accessing sensitive information or IT assets. This means that minimal permissions will be used, and only when required. Separation of duties shall be enforced (role-based access scheme shall be coordinated through and enforced by the AO; currently designated through the SID IA Office).

5.6.3.12 Data Access Rights

In accordance with DoD Instruction 8500.01 (Reference (y)), the contractor shall support the use of encryption, access control, user identification and authentication, malicious content detection, audit, and physical and environmental control to ensure the confidentiality, integrity, availability, authenticity and non-repudiation of all DARPA data and information.

5.6.3.13 Shared File Services

The contractor shall provide users with access to Shared File Services via the network to store and retrieve files with controlled access that complies with the Government's access management policies. All file servers, Storage Area Networks, or Network Attached Storage solutions providing shared file services will include access controls, backup and recovery services in accordance with SLO 2.6. The Government currently imposes no quotas for users on file storage.

5.6.3.14 Service Continuity Management

In order to provide Service Continuity Management, the contractor shall provide Backup and Restore Services, Disaster Recovery Services and Continuity of Operations (COOP) support services commensurate with DARPA's MAC III designation and in accordance with DoD 3020.26 (Reference (t)). While DARPA is a MAC III organization, day-to-day service continuity is extremely important to DARPA's successfully completing its mission; therefore, the contractor shall plan for redundancy and high levels of availability outside of the disastrous event. SLOs 2.1 through 2.9 apply.

5.6.3.15 Backup and Restore Services

The contractor shall provide backup and restore services to include on-site and off-site storage of Government-owned media containing backups of data and files, as well as documentation and training for Government personnel on the procedures for restoration. All backup and restore policies are subject to Government approval and DoD guidelines (Reference (e)). The contractor shall comply with Service Delivery SLO 1.5. The contractor shall perform, at a minimum, the following Backup and Restoration activities:

a. Execution and verification of the backups of all production servers. All servers shall have the backup client and all associated patches installed
b. Complete regular test restores of files and entire systems to verify the quality of the backups as well as the procedures for completing restores
c. Create and maintain system state backups of all relevant servers
d. Generate SOPs associated with the Backup and Restore processes and perform periodic tests to restore/build the service or systems in event of failure
e. Provide client-level, automated, continuous backup with little or no impact on user performance or network workload—with instant recovery of all system information
f. Provide Government-approved commercial space for the retention of backup and storage media

5.6.3.16 Disaster Recovery Services

The contractor shall provide disaster recovery planning through on-site and off-site storage of Government-owned media containing backups of data and files, as well as documentation and training for Government personnel on the procedures for restoration. All disaster recovery is subject to Government approval and DoD guidelines (Reference (e)). The contractor shall plan and conduct tabletop drills in coordination with the Government. The contractor shall plan for redundancy and quick failovers for all production servers, applications and services to provide maximum uptime in accordance with SLO 2.6. The servers and services shall be categorized as follows:

a. DARPA Mission Critical Servers and Services
    i. These servers will be included in an Continuity Of Operations Plan (COOP) (if created) as a phase one
(b)(1)
(b)(1)
    ii. These servers and services may include, but are not limited to, E-mail, Blackberry, calendaring, VPN services, etc.
b. Critical Servers and Services

i. These servers and services will be in phase two of a COOP plan (if created)

(b)(1) [redacted]

ii. These servers and services may include, but are not limited to, external connectivity to non-DARPA organizations

c. Non-Critical, but Essential, Servers and Services

i. These servers and services will be in phase three of the COOP plan (if created)

(b)(1) [redacted]

ii. These servers and services may include, but are not limited to, Inventory databases, historical/archived data and/or external connectivity to non-DARPA organizations

5.6.3.17 Continuity of Operations Plan (COOP) Support

The contractor shall have the capability to support the creation of an IT Continuity of Operations Plan (COOP).

5.6.3.18 Standard Application Support

Standard Applications that are in production in the DARPA environment shall be maintained by the contractor through Software Distributions of new versions and appropriate upgrades and patches. If the application has an associated database, database support shall also be provided for all standard applications.

5.6.3.19 Software Distribution and Upgrades

Contractor shall provide, for all standard applications support to the end-user, an automated method or tool (currently in use is SCCM) for software distribution and upgrades. Application distribution and upgrades will be, as much as possible, transparent to the users. Software distributions due to Vulnerability Announcements shall comply with SLOs 4.2 through 4.4. Other software distributions and upgrades will be completed by the Government designated deadline per SLO 5.3.

5.6.3.20 Database Support

Standard applications requiring back-end databases shall be maintained by the contractor, who shall designate database administrator(s) to perform routine maintenance to include, but not limited to:

a. The creation and testing of backups to ensure that the database can be recovered in the event of a failure
b. Verify and maintain data integrity
c. Define and/or implement access controls to the data
d. Maintain database availability by ensuring maximum uptime through non-disruptive updates or a redundant environment, such as a clustered database server farm
e. Maintain database performance by ensuring maximum performance and capacity through monitoring
f. Assistance with development and testing support by helping programmers and engineers to efficiently utilize and access data in the existing databases

5.6.3.21 Web Hosting Services

The contractor shall provide web hosting as a service for DARPA websites, including storage and processing of web content. This service includes DARPA internal access, public access, and unclassified hosting. Identification and Authentication (I&A) and Access Control to DARPA as well as to DARPA and DoD secure websites will occur via DoD PKI in compliance with communications tasking orders (JTF-GNO CTO) for PKI. As part of this service, the contractor shall provide statistics and reporting regarding web access and availability in accordance with SLO 2.6. The service does not include authoring of web content and application development, although those services may be ordered from the Service Catalog/DARPA Store Front, or through a Professional Services project.

5.6.3.22 Web Support Services

The contractor shall provide webmaster, web analysis, and maintenance services. The contractor shall have a webmaster role on the task order for providing day-to-day support of existing and new basic websites and pages for users, including DARPA.MIL. The webmaster shall ensure that all the links on DARPA websites (internal and externally) are working properly and compliant with Rehabilitation Act of 1973, section 508 (Reference (s)) requirements. The webmaster shall track the traffic going to a website. The webmaster controls the security of the website, so that hackers cannot access sensitive data. Additionally, the webmaster shall improve the performance of existing websites, which includes optimizing the website and analyzing the speed of the website.

a. The Webmaster shall have experience with Content Management System (CMS), specifically Ektron CMS would be preferred
b. The webmaster should have good command over HTML (Hypertext Markup Language), CSS (Cascading Style Sheets) and Extensible Markup Language (XML)
c. The webmaster shall have experience with web applications such as Adobe Dreamweaver. The webmaster shall ensure interoperability for all kinds of browsers, e.g., Internet Explorer, Mozilla Firefox, Safari, etc.

5.6.3.23 Legacy Systems Support (Critical Applications)

The contractor shall ensure desktop access and provide enterprise infrastructure services for critical legacy applications as directed by the Government.

5.6.3.24 Customer Services Support

The Customer Service functional area focuses on the “customer facing” aspects of supporting the services provided to the Users under this task order.

5.6.3.25 Help Desk Support Center

The contractor shall provide a centralized Help Desk Support Center as a single point of entry for Users to receive support. As necessary, the Help Desk will route calls to other Organizational Help Desks. Users shall have multiple methods for contacting the Help Desk for support (web forms, email, and a phone call). The contractor shall provide User relationship management services as detailed in the following sections.

The **Help Desk Manager** shall be responsible for the unclassified IT Help Desk Operation. The Help Desk Manager shall oversee personnel, manage coverage, ensure all standard operating

procedures are current and followed, manage incident and problem resolution as well as Knowledge Management resulting from resolved tickets. This position is directly responsible for the reporting of Help Desk metrics to the Program Manager.

The Customer Relationship Manager (CRM) shall act as a liaison between end-user customers and the contractor, meet weekly with the COR, and is the Government point-of-contact for tasks related to customer relations.

The Ad-Hoc/SME Support Analysts' (2) two positions are senior Help Desk analysts who are responsible for responding to broad-scope, high-profile issues and executive personnel.

5.6.3.26 Self-Help Support

The contractor shall provide user-accessible, self-help tools and capabilities that are designed and maintained to address IT inquiries and incidents without users having to formally place Help Desk calls. The contractor tools and capabilities shall include a searchable knowledge repository providing User access to FAQs and a library of commercially available and DARPA custom knowledge documents encompassing all DARPA User Configuration Items.
The contractor shall provide, at a minimum, the following:

a. A knowledge repository that includes a searchable library of relevant IT policy and administrative documents
b. Tools and capabilities which enable Users to check the status of their Help Desk Ticket(s)
c. Tools and capabilities which provide Users with updates regarding the current status of network services, planned outages, and other IT- related notifications
d. The monitoring and review of the effectiveness and usage of self-help tools and capabilities for service improvement analysis
e. The development of recommendations for improvement to self-help tools and capabilities as requested

5.6.3.27 Contractor Service Level Support

The contractor shall provide end-to-end life-cycle management of all Help Desk customer service requests facilitating the effective hand-off between support Tiers, as follows:

a. Tier 1 provides support as to the features, functions, and usage of in-scope hardware and software (traditionally called answering support, initial diagnosis, and triage) and may be transitioned to other personnel for desk-side support
b. Tier 2 provides support for issues that are more technical or specialized in nature and are the result of an escalation procedure from Tier 1 (escalation within the Help Desk or transitioned to other personnel for desk-side support). Note: Users will have the ability to request Tier 2 support in initial request, or any time thereafter
c. Tier 3 provides support for incidents that cannot be resolved in Tiers 1 and 2 (escalation to other functional groups, subject matter personnel, third parties or transitioned to other personnel for desk-side support)

5.6.3.28 Help Desk Services

The contractor shall provide an on-site Help Desk based on industry best practices with Government-centric, courteous, responsive and knowledgeable technical assistance for solving information technology service-related issues to the User's satisfaction. The contractor shall plan to have sufficient coverage to answer all calls within three rings. The contractor should expect a number of Help Desk tickets commensurate with the industry standard for exemplary support of ~1300 Users—incumbent averages between 2700-3200 requests per month. This includes providing an integrated service with a single point of entry for all DARPA Users. The contractor shall provide knowledgeable analyst support in order to maximize first call resolution (SLO 6.3). Best practices include, but are not limited to the following policies:

a. Help Desk analysts shall retain "ownership" of each request they open until its resolution, including managing ticket escalation, providing follow-up, and regularly notifying Users as to ticket status
b. The contractor shall ensure Help Desk analysts are current on the latest Government-relevant IT Government Service and technical training
c. The contractor shall meet Government expectations by setting and adhering to promised schedules
d. Re-opened tickets shall be tracked and Trend Analysis shall be performed and reported in accordance with SLO 1.6
e. U.S. Persons and privacy information shall be protected; and
f. A Help Desk Operations Manual shall be developed and maintained covering support requirements, Standard Operating Procedures and appropriate checklists

The Help Desk shall provide basic support to DARPA visitors attempting to access the wireless services provided on the 1st floor only. Visitor Support Services shall be provided from 8:30 am to 7 pm, Monday through Friday.

In addition, Help Desk services shall include mid- and senior-level support for service requests that extend beyond the basic Government services and problem resolution associated with Help Desk support. These service requests shall be supported and documented within the HDMS. Examples of these types of service requests include, but are not limited to, the following:

a. Virus scanning of disks
b. Burning of CDs
c. Data copies/moves/conversion/organization/migration
d. SW/HW installation and re-configuration
e. Initiation of the file restoration process (SLO 1.5)

The contractor shall provide escalation services with procedures to be reviewed and approved by the Government and implemented by the contractor. These services shall include the timely notification of Government personnel by the Help Desk of planned or unplanned system maintenance or degradation of Government's information technology services. Because Help Desk service is mission-essential for the DARPA User community, the contractor must provide ongoing training to Help Desk personnel in order to maintain a high caliber of service and support.

For the purposes of this PWS, the term trouble tickets or tickets will be used to refer to Help Desk Tickets that have not yet been classified as a Service Request, Incident, MACD, etc. Service Requests align with the Service Delivery SLOs. Incidents are trouble tickets where the problem that the User is experiencing is preventing them from doing their job. Incidents align with the Incident Management SLOs.

5.6.3.29 Help Desk Management System (HDMS)

A Help Desk Management System (HDMS) shall be employed. The contractor shall use, manage, patch and upgrade the Government-owned Remedy system. The HDMS shall be used to develop and maintain a knowledge base of all Help Desk Tickets, including resolutions. The HDMS shall include an audit log of all changes. Contractor shall develop and submit to the Government for approval a HDMS User interface design and data dictionary to ensure that all desired information is captured. The HDMS shall allow write privileges to Government specified personnel; read privileges shall be made available at the Government's discretion to personnel for validation and verification activities.

The contractor shall record non-IT and out-of-scope incidents, requests, and other out-of-scope contacts in the Help Desk Management System and redirect them to the appropriate DARPA office per Government policy.

5.6.3.30 Knowledge Management System Support

The contractor shall provide input to the Government-owned Knowledge Management System (KMS) for documenting solutions to resolved Help Desk Tickets where commercial knowledge documentation does not exist or does not address the incident. The contractor shall use the Government-owned Remedy system. Issues and solutions shall be added to the KMS knowledgebase and made available to users as self-help support within five business days of incident closure.

The contractor shall inform users of the status of their tickets through the following methods:

a. Phone calls,
b. E-mail responses, and
c. A web-based portal that offers self-serve access to real-time ticket status information and allows for user feedback.

The contractor shall provide updates to the user upon any change in the ticket. The contractor shall maintain all ticket data for the life of the task order and provide synopsized reports upon request. The contractor shall provide all ticket data in an easily portable format that maintains any relational information. Data shall be provided within one hour of request in a portable data format approved by the Government. The contractor shall further provide comprehensive Help Desk statistics and trends as part of the Weekly Activity Report (WAR), and forward tickets that are open longer than five days to the Government for review.

5.6.3.31 User Training

The contractor shall develop and document training requirements that support the ongoing provision of Services, including training on new service or application functionality.

The contractor shall provide training when substantive technological changes (e.g., new services or functionality) are introduced. For each change in services and/or applications, the contractor shall analyze, identify, and implement the form of training most effective and efficient for DARPA Users. Types of training are expected to include: desk-side, formal classroom and on-line computer- based training (CBTs). Space for classroom-based User training will be provided by DARPA in Government or contractor-occupied facilities. Hardware, software, equipment, training materials, and supplies necessary for effective training shall be provided by the contractor. Automated User training solutions used by the contractor shall incorporate advanced distance learning solutions. User training and updates to relevant documentation (including SOPs, FAQs, etc.) for the use of a Configuration Item shall be made available as a result of any of the following:

a. Initial Implementation
b. Implementation of a change in technology or User interface
c. Identification of User knowledge shortfall (e.g., as a result of a Help Desk call or User-invoked systems failure)
d. Trend Analysis performed on Help Desk tickets
e. Move/Add/Change/Delete
f. Upon COR request

5.6.3.32 Standard Integrated Office Automation Software Suite

The standard integrated software suite shall include at a minimum, email, word processing, spreadsheet, presentation graphics, project management, database, calendaring, a collaborative work environment, forms processing, browser, and virus protection tools. The Microsoft Office suite is preferred. The software suite shall provide the capability to view, hear, manipulate and manage information consisting of text, graphics, images, video, and audio. This shall also include processing and rendering of the multimedia data being transferred from any source. COTS software to support advanced and/or specialized functions beyond those provided as standard office automation tools shall be available and may be purchased separately from the Service Catalog / DARPA Store Front.

5.6.3.33 Desk-Side Hardware Services and Maintenance

The contractor shall provide support for multiple hardware configurations, to include, but not be limited to, Dell, Sony, and Apple (Mac OS) computers. The contractor shall ensure hardware configurations are integrated with security devices.

In order to meet the Government's mission, the contractor will work with the Government to define technologically advanced desk-side hardware packages to meet, if not exceed, the expectations of Government personnel for advanced support. The contractor shall repair, support and refresh all desk-side and public access area hardware, to include, but not limited to:

a. Laptops, Desktops
b. Monitors
c. Keyboards and mice
d. Docking stations
e. Printers

f. Copiers
g. Conference Room Audio/visual equipment
h. Mobile Devices – currently available wireless PDAs are Blackberry, iPhone, and Samsung S4 devices. Hardware bundle should include the devices, with telecommunications services already activated, wall chargers (2), car chargers, hands free (non-blue tooth) headsets and carrying case
i. Tablets/Mobile Workstations (e.g., Windows-based, iPads, and Kindle devices)
j. Network cables

Desk-side hardware configurations will be bundled together per guidance and approval from the CCB and made available in the DARPA Store Front for Government personnel to choose based on their individual requirements. Based on the technology refresh guidelines set forth by this PWS or from the CCB, the contractor will purchase hardware warranties commensurate with the expected lifecycle of the equipment. Based on the requirements outlined in the SLOs, the contractor shall repair or provide an interim solution until the hardware can be repaired or replaced.

The staff supporting the desk-side hardware services and maintenance tasks will participate in the asset management process and a status of all desk-side hardware inventories should be accessible to the Government and its designees via web or other reporting mechanism in near real-time.

5.6.3.34 Conference Room (A/V Equip) Support

The contractor shall provide support to DARPA's conference room facilities. Conference Room facilities that also require Video Teleconference capabilities shall comply with the DoD Risk Management Framework (RMF). The contractor shall support Video Teleconferencing in all designated conference rooms in accordance with SLO 2.8.

5.6.3.35 Client-side Application Support

The contractor will provide the first line of support for all client-side applications to include but not limited to:

a. Legacy Applications – The contractor shall continue to support all systems which are currently in use in the DARPA enclave. The contractor shall provide data interface and enterprise infrastructure service for legacy applications
b. Government Applications – The contractor shall provide client-side support for all Government applications that are required by Government personnel. This may include but is not limited to the Defense Travel System, HR payroll, etc.
c. Office Automation Applications (e.g. Microsoft Office 2007/2010, Anti-virus, etc.) - The contractor staff shall be fully trained to support the use of and the troubleshooting of the Office Automation suite of applications that possess a Certificate of Networthiness. Updates and upgrades of these products will be completed by the Operations team and be transparent to the users
d. Specialized applications (e.g. AutoCAD, MATLAB, etc.) – All COTS software that supports specialized project needs beyond those provided by the standard office automation tools shall be made available after going through the IA approval process (e.g. as a general rule, freeware cannot be installed on Government-issued computers). Once an application has been approved it will be added to the Service

Catalog/Store Front and licensing will be tracked via the Asset Management process

Client-side applications in addition to the client-side office automation applications are provided as a baseline configuration to all desk-side Users, include, but may not be limited to, the following:

a. Operating System
b. PDF Reader/Writer
c. HTML Editor
d. Web Browsers
e. Forms
f. Antivirus
g. Viewer/Converter (e.g., Quick View Plus)
h. File Compression (e.g., WinZip)
i. Backup Solution
j. Video Player (e.g., Quick Time)
k. Sound Player l.
Image Viewer
m. DVD Software
n. DVD/CD Writer
o. Personal Firewall
p. Hard drive encryption – currently only on portable computers

5.6.3.36 Wireless PDA Configuration Item

Wireless PDA Configuration Item shall include hardware, software, global position system and telecommunications services necessary to provide the ability for DARPA Users to transmit and receive secure electronic mail with attachments through a wireless medium from any location in the continental United States, as well as outside the continental United States, where available (e.g., Europe, the Middle East, and Australia). The Wireless PDA Configuration Item shall also include the ability for DARPA Users to transmit and receive voice services from any location in the continental United States in accordance with DoD Directive 8100.02 (Reference (c)). The Wireless PDA Configuration Item is comprised of the hardware, software, security features and services provided to DARPA Users as resources, such as:

a. Blackberry PDA (can send and receive voice and e-mail)—the Government currently uses the Blackberry Enterprise Server (BES).
b. Apple iPhone (can send and receive voice and e-mail)—the Government currently uses Good Technology for electronic mail on the iPhone
c. Samsung S4 (can send and receive voice and e-mail)—the Government currently uses KNOX to secure electronic mail on the device

5.6.3.37 Printer Configuration Item

The Printer Configuration Item is comprised of the hardware, software, security features, and services necessary for DARPA Users to perform either local or network printing functions. Printer Configuration Items must be compatible with all data-related capabilities provided by the contractor. The contractor shall electronically monitor departmental printers to provide proactive

service. All consumables associated with the proper functioning of printers other than media (paper, labels, and transparencies) shall be provided by the contractor. Printer consumables include, but are not limited to, toner, drum replacement, fuser assemblies, transfer assemblies and paper rollers. The Printer Configuration Item shall be proposed by the contractor to the Government, and will be reviewed and approved by the Configuration Control Board (CCB). Printer capabilities shall be state of the shelf. All printers must comply with the following minimum specifications and other requirements without modifications:

Minimum Printer Specifications:

	Personal Printer (Inkjet)	Personal Printer (Laser)	Departmental Printer (B&W)	Departmental Printer (Color)
Network Capability	Yes			
Duplexing	Yes			
Speed	15 ppm B&W; 11 ppm color	35 ppm	62 ppm	42 color ppm
Paper-tray capacity	250 sheets	250 sheets	1000 sheets	700 sheets
Print Quality/ Resolution	600 dpi B&W;1200 dpi color	1200 dpi	1200 dpi	1200 dpi
Usage Rating	7,500 pages per month	10,000 pages per month	150,000 pages per month	65,000 pages per month

5.6.3.38 Copier Configuration Item

The Copier Configuration Item is comprised of the hardware, software, security features, and services necessary for DARPA Users to perform local scanning and copying and network printing functions. Copier Configuration Items must be Common Access Card enabled and compatible with all data-related capabilities provided by the contractor. For the purposes of this section, although unclassified copiers will have network printing capability, they will be referred to as copiers. The contractor shall electronically monitor departmental copiers to provide proactive service. Printer consumables include, but are not limited to, toner, drum replacement, fuser assemblies, transfer assemblies and paper rollers. The Copier Configuration Item shall be proposed by the contractor to the Government, and will be reviewed and approved by the Configuration Control Board (CCB).

All copiers must be digital and comply with the following minimum specifications and requirements without modifications:

a. All copiers must be equipped with non-resettable copy meters. Copiers must be programmed to give separate copy counts for both black and white, and color copies.
b. Both the number of paper feeds and the total paper capacity must be simultaneously available on-line. Also the paper capacity must be exclusive of any by-pass feeder.
c. All copiers must copy, scan, email, and print.
d. Console display must signal the operator of the need for paper, toner, developer / dispersant or of the occurrence of paper jams. Controls must also include exposure adjustments. Console display must enable end users to easily replace consumable components including toner, staples and paper.
e. All copiers must be ENERGY STAR compliant.

Minimum Copiers Requirements:

	Customer-facing Copiers	**High Speed Copier/Print Press**
Automatic Document Feeder (ADF)	▪ Automatic Tray-less Duplexing (2-sided printing) ▪ 100-sheet minimum automatic duplication document feeder ▪ Feeds 5.5 x 8.5 inches up to 11x17 inches, minimum paper thickness of up to 110lb cardstock ▪ Mixed size originals	▪ Automatic Tray-less Duplexing (2-sided printing) ▪ 100-sheet minimum automatic duplication document feeder ▪ Feeds 4 x 5.6 inches up to 11x17 inches, minimum paper thickness of up to 110lb cardstock ▪ Mixed size originals
Paper Tray Capacity	▪ One bypass tray 100 sheet minimum ▪ 4 user adjustable trays, 8 ½ x 11 in min up to 11 x 17 in	▪ Automatic switching paper trays ▪ 3 standard loading trays (user adjustable trays 8 ½ x 11 inches up to13 x 19 inches) ▪ 2 High-capacity trays (8 ½ x 11 inches minimum up to 11 x 17 inches ▪ One bypass tray 100 sheet minimum
Paper Media Types	▪ 20lb Plain GSA recycled paper products ▪ 18lb. bond – 110lb. cover, uncoated ▪ 28lb. bond – 110lb. cover, coated ▪ Transparencies, Stickers, Labels, High-Gloss media	
Reduction & Enlargement Functions	▪ Automatic and Manual ▪ Image reduction/enlargement presets 25% to 400% with optional 1% increments	
Programming Options	▪ None	▪ Job Build/Store/Recall ▪ Automatic job recovery ▪ Tab creation and insertion ▪ Slip sheet insertion ▪ Cover insertion
Speed	▪ Print/Copy/Scan 60 ppm (B&W); 55 ppm (Color)	▪ 55 ppm full color; 60 ppm black and white
Print Quality/ Resolution	▪ 600 x 600 dpi color resolution	▪ 2400 x 2400 dpi or equivalent high-resolution color for sharp images, photographs, crisp, clean text, gradients and fine detail ▪ Black and white 2400 x 600 dpi at 256 grayscale

Finishing Options	▪ Sort and collate/offset collate
	▪ Multi-position stapling (50 sheet minimum)
	▪ Hole-punching (2 and 3-hole)
		▪ Sort and collate/offset collate (Offset Stacker)
		▪ Multi-position stapling (50 sheet minimum)
		▪ Hole-punching (Interchangeable dies)
		▪ 2 and 3-hole
		  ▪ Spiral punch (twin-loop 21 and 32-hole)
		  ▪ Plastic comb punch (19-hole)
		▪ Multi-folding (Bi-fold, Tri-fold, C-fold, Z-fold, Tabloid Z-fold, Gatefold desirable)
		▪ Booklet-making w/trimmer (32 sheet minimum)
		▪ Saddle-stitching w/face edge trimmer (32 sheet minimum)
		▪ Alpha/Numeric Bate Stamping/Watermarking

	Customer-facing Copiers	**High Speed Copier/Print Press**
Network Capability	▪ Desktop Printing ▪ Scan-to-email/file (JPEG, PDF, TIFF)	▪ Desktop Printing ▪ Print Controller (e.g., Fiery) with screen preview, add, edit, or delete pages, merge fixed or mixed pages ▪ Job Scheduling ▪ Job Archive Scan-to-email/file (JPEG, PDF, TIFF)
Power Requirements	▪ 120 volts/20 amps	▪ 120 volts/30 amps Additional finishing modules: 120 volts and 20 amps
Section 508 Compliance	▪ Two (2) copiers are to meet Section 508 compliance standards for wheelchair accessibility. Accessibility measures required for disabled personnel are assisted document lid lift, angled console, and footswitch.	▪ None

Estimated Usage:

The average monthly number of prints for each machine type is set forth below.

Copier Type	Estimated Monthly Volume	Total Average Monthly Pooled Volume
Customer-facing Copier	1,200 (Color)/820 (B&W)	49,200(Color)/33,620 (B&W)
High Speed Copier/Print Press	70,000 (Color)/30,000 (B&W)	70,000 Color)/30,000 (B&W)

Maintenance and Repair:

In the event of a copier/printer breakdown:

a. Maintenance technicians shall be available on-site within eight (8) hours (excluding holidays and weekends).
b. The two High Speed Copier/Print Presses are deemed "critical" to the DARPA mission. In the event of a breakdown, a tier-2 technician shall arrive within four (4) hours (including holidays and weekends), fully capable of diagnosing the problem and, to the maximum extent practicable, making any necessary repairs. In the event both copiers breakdown at one time and repairs cannot be completed promptly, the contractor shall provide an alternate solution to complete outstanding jobs.
c. A loaner copier of similar make and model shall be provided by the contractor for copiers/printers which cannot be repaired and are not in good working condition within three (3) business days of the service request. Repair of broken copiers/printers must be completed within 14 business days.
d. Only Certified and Factory Trained Service Technicians will be utilized.
e. Use of 100% original equipment manufacturer (OEM) parts for maintenance and repair of copier is required. All copiers will be equipped with or supplied with original equipment manufacturer (OEM) recommended surge protectors, appropriate adapters, and will be properly grounded.

On-Site Training:

A minimum of two (2) initial training sessions for DARPA personnel shall be conducted at DARPA upon equipment installation with the schedules, participants and number of participants per session identified by DARPA. Two (2) subsequent training sessions per year shall be available at DARPA on a scheduled basis during the task order term for purposes such as training of new personnel, providing refresher sessions, increasing user productivity through effective use of networked features or providing assistance with new procedures or equipment. Training shall also be available on an as needed basis via the Help Desk.

Security Requirements:

For all copiers:

a. Software that can conduct a DoD overwrite must be installed. The Government has the option to buy-back any or all drives which might have been contaminated
b. There must be a fail-safe condition for overwriting so that if overwriting is interrupted, it fails to a known safe state and overwriting may resume later
c. All copiers must have necessary software and/or functionality to detect, prevent, and log the copying of currency
d. Unneeded network services must be disabled
e. Networked devices must be secured
f. Access Control List (ACL) capability is desired to restrict who can access specific functions (e.g., limit by IP address who can print, who can administer the device, etc.)

For copiers in classified areas:

a. No network connectivity is required, and if possible disabled.
b. There must be a written contamination mitigation strategy (clearing memory, clearing images, clearing media/hard drives, etc.)
c. There must be proper handling and storage of physical media
d. There must be clear labeling (e.g., "Unclassified Use Only") and specific approval to use at a particular classified level
e. Equipment used for maintenance of classified media remains at the classification level of that media. (Laptops used to access a classified copier hard drive becomes classified, and vendor may not take it back out of the facility)
f. There must be a mechanism to allow hard drives on classified copiers to be destroyed (by DARPA) or remain at the DARPA facility. Once contaminated with classified material, hard drives may not leave the DARPA facility. Copiers in classified areas that are returned for repair or retired shall be returned without their hard drives
g. If the copier is attached to a need-to-know restricted classified network to be used as a copier, the copier must have appropriate mechanisms or procedures to ensure that only the person who printed the document may retrieve the document. Examples of need-to-know restricted networks include SAP and SCI, or collateral networks where need-to-know has been invoked. Acceptable control mechanisms include requiring a PIN before the job is printed, or securing the copier manually.

Technological Environment Requirements:

a. Network Interface: Standard Ethernet 10/100 BaseT
b. PDL/PCL: PCL SE/6, Postscript 3
c. Network Printing Capabilities, Support Windows 2008r2 print server
d. Scan and Email Capabilities
e. Integrate with Microsoft Exchange 2010 e-mail and fax capabilities image
f. Secure Overwrite Software compatible—inoperable drives that cannot be overwritten shall be returned to DARPA for destruction. Contractor shall overwrite, certify, and label the storage media prior to removal from the Agency. The Government will have the option and right to buy back the storage media if desired.
g. Authentication for scanning option
h. Integrate with Active Directory for LDAP lookups for e-mail addresses
i. No wireless connectivity is allowed, if present must be disabled and not configurable by end users.
j. Storage media that is replaced shall be overwritten in accordance with the above. The Government will have the option and right to buy back the storage media if desired.

Partner Applications & Interface Requirements:

The contractor shall provide copier management software (Netaphor is currently in use) to conduct copier fleet site audits.

a. The copier management software shall be compatible as a copier lifecycle management solution. It shall be business process software dedicated to reducing the total cost and managing service performance of copier assets.
b. The copier management software shall be a comprehensive and easy to use copier management tool. Software must have an innovative discovery mechanism that builds an inventory of all networked and directly connected copiers without the use of any additional desktop agents.
c. The copier management software shall allow print counts, page counts, error statistics, and usage and service analytics for assessment and fleet management.
d. The copier management software shall collect utilization and cost data by copier and location, as well as provide notification by incident type and location to reduce help desk calls, track downtime, and resolution time in order to improve service performance.
e. The copier management software shall have a metering function for automated collection of print count statistics for efficient remote meter reading.
f. The copier management software shall allow for the capability of daily, weekly, monthly or customized date and time meter reads. It shall provide reports of collected data in industry standard formats

5.6.3.39 Desk-Side Technology Refreshment

The contractor shall make every effort to ensure minimal impact to the User during refreshment, insertion and enhancement activities. For DARPA devices, the contractor shall minimize

downtime; if the device is the User's primary workstation, the contractor shall offer a temporary device for use while the primary workstation is unavailable. Additionally, the contractor shall ensure the accuracy of data transfer and carryover: desktop icons shall be restored to the same locations, printers and drivers re-installed, personal and business files transferred, and applications re-installed. The contractor shall transfer data for wireless devices in the same manner. Refer to section 5.6.2.6 Technology Refreshment, Insertion and Enhancement for the technology refreshment guidelines. External hardware peripherals and software products acquired through the COTS Catalog and compatible with the refreshed Configuration Items shall be migrated to the refreshed devices. If any internal components, external hardware and/or software products are determined to be incompatible or not standard (i.e. a larger hard drive) within the refreshed device, the contractor shall offer the DARPA end-User alternative solutions which provide similar or better functionality through the DARPA Store Front. The contractor shall update the inventory information in the asset inventory database upon completion of the technology refreshment within four hours in accordance with SLO 5.2.

5.6.3.40 User Outreach

The contractor shall perform proactive communications and outreach with DARPA Users to inform them about services provided in this PWS. The contractor shall provide current informational materials such as brochures, briefings, seminars, white papers, flyers, FAQs, web content, etc. targeted to DARPA Users. The contractor shall conduct information exchange sessions (e.g., Town Halls and focus groups) in conjunction with the COR as required to provide information and receive User feedback about the information technology services provided under this PWS in accordance with SLO 6.1. The contractor shall draft Customer Notifications for COR approval informing users of service activities or outages that may impact them. The contractor shall employ Government-approved templates for standard, recurring situations. The contractor shall form a supportive and close working relationship with other DARPA contractors performing work impacted by or related to this PWS. The contractor shall also send out User satisfaction surveys to be completed by the Users within one week of ticket closure; User satisfaction surveys shall be used in accordance with SLO 6.1.

5.6.3.41 Request Fulfillment

Request fulfillment focuses on Service Requests that are also "standard changes" but do not go through the Change Management process. An example of this type of request would be a manager requesting a new standard workstation configuration for a new employee. While it is a change, it does not need to go through the full change management process. Service Requests follow the predefined request fulfillment process, which is built around a list of standard changes (a.k.a. services). If a service request is made that is not a standard change then it must go through the formal change management process. Service Requests should be fulfilled in accordance with SLOs 1.1 and 1.4.

5.6.3.42 Moves, Adds Changes, and Deletes (MACDs)

For User requested MACDs, the contractor shall provide services to perform system hardware and software changes of data, video conferencing center, printer, and/or wireless devices. MACDs include the following:

a. De-installation, move, re-installation, or change of Hardware Configuration Items
b. Creation, modification or deletion of a User account including telephone numbers, e-

mail and directory services
c. A change in type of device
d. A contractor periodic or unscheduled software refresh or update.
e. Application of appropriate security features

5.6.3.43 Inventory / Asset Management Updates
The contractor shall update the inventory information in the asset inventory database following any MACD service within four business hours, in accordance with SLO 5.2.

5.6.3.44 Service Catalog / Store Front
The contractor shall provide a Service Catalog of hardware, software, support services and other COTS items to be ordered and funded as needed to meet DARPA's need for specialized or advanced functionality.. Items listed in the catalog shall be pre-integrated and available for immediate access when ordered to augment services, or available for pilot purposes when ordered in conjunction with Professional Services tasks. All items in the catalog shall be integrated and interoperate with all services upon deployment.

The contractor shall provide an electronic ordering system as the front-end to the Service Catalog referred to as the DARPA Store Front that allows DARPA Users to select hardware, software and services necessary to perform their computing functions. This ordering system shall be a contractor provided, Government approved, web-enabled catalog with multiple approval levels. The Service Catalog shall publish alerts, via e-mail, to all appropriate parties as order status changes. The Service Catalog shall have the capability of generating live reports including financial reports by time, status and office. If a Configuration Item in the Service Catalog must be procured, then SLO 1.2 applies.

The contractor shall comply with the Service Catalog procedures provided by the Government and implemented by the contractor. All Service Catalog related documents created by the contractor relating to processes and procedures under the task order are owned by the Government. As such, the contractor must allow and provide capabilities for authorized Government managers and staff, as well as designated contractors, access to such documents. Authorized DARPA Staff and contractors shall have full and unrestricted access to such documents. The contractor shall provide these services in accordance with the requirements in the following subparagraphs to achieve the highest level of operational flexibility and User satisfaction.

5.6.3.45 COTS Catalog Services
The contractor shall provide COTS Catalog services via the DARPA Store Front to allow for the purchase of approved and integrated software, hardware and services. The contractor shall make available support services for all COTS items to include installation, initial training, warranties and Help Desk support. The contractor shall provide users with the capability to select and bundle software, hardware and services as the User requires.

5.6.3.46 COTS Catalog Maintenance
Addition and removal of items from the Catalog as well as changes in cost shall be upon the approval of the COR. COTS Catalog pricing shall be adjusted annually, at a minimum. Any item that is ordered once shall by default be automatically entered into the COTS Catalog, upon

approval from the CCB. For all new COTS items, the contractor shall include an associated support services line item in the catalog. This item shall provide the annual cost of supporting the new item. The contractor shall update the catalog and the Property Asset Tracking System to include the new items. The contractor shall also ensure obsolete items are removed on an annual basis, at a minimum. In the event of a COTS catalog order cancellation, the contractor shall, in conjunction with the Government, determine if the item(s) should be returned to the original vendor or retained as an in-stock item. If the item is returned, the contractor and the Government will determine an equitable adjustment to be reflected on the contractor's invoice. If the item is retained, its disposition shall be reflected on the Asset /Credit report, and it shall be available to the Government until it is fully depreciated. Unless there is a reasonable likelihood a returned/cancelled item will be needed by someone else in DARPA before the item is fully depreciated, it shall be returned to the vendor (unless it is "non-returnable"). This decision shall be based on how many similar/same items are currently being used, how often the items are ordered, the number of the items already in stock and how long they have been in stock, and other best practices applicable to inventory management.

5.6.4 Professional Services

Professional Services shall be provided by the contractor on an as needed basis for one-time or first-time projects to meet emerging Government requirements. Each request for Professional Services will become a project that is managed according to the definitions and processes defined in the following sections.

5.6.4.1 Professional Services Work Categories

The contractor shall provide qualified expertise that falls under the professional services categories listed below.

a. Category 1: Advanced Windows System Integration and Servers Application Support
b. Category 2: Advanced Non-Windows Systems Integration, Applications and Servers Support
c. Category 3: Application Analysis, Design and Programming Support
d. Category 4: Emerging Technologies Research Support
e. Category 5: Testing and Implementation of IT R&D Emerging Technologies
f. Category 6: Surge Support

5.6.4.2 Professional Services Projects

Professional Services (PS) Projects begin with requirements from a customer request through the Service Catalog. Contractor personnel are responsible for initial requirements gathering. If the request is approved by the COR, a work assignment, or statement of work (typically between 1 and 3 pages), will be prepared and provided to the contractor. The contractor shall prepare a Cost and Technical proposal in response within five (5) business days—if additional time will be required to prepare the proposal, the contractor shall notify the COR within one (1) business day. Individual staff or subcontractors will be proposed by the contractor in response to a Project Request (PR) on an as needed basis. The contractor must identify the work categories and provide detailed resume(s) with references with its proposal as evidence that the proposed staff is qualified to do the work. The Government will determine if the proposed staff is qualified, to include contractor-led project management. The Government may refuse to accept proposed staff

and may request the contractor propose alternative staff. Once the staff is accepted, the contractor may only draw from the pool of acceptable staff. COR approval is required if the submission of the proposal is expected to take more than ten (10) business days. All PS Projects shall be limited in scope and duration with COR-approved schedules and resource/personnel plans. Once a project is underway, changes in scope, deliverables, and time (completion date), may only be modified with consent of the COR. Project Change Management and Change Request processes shall be utilized. Any changes in personnel during the project must be approved by the Government. SLOs 7.1 and 7.2 apply.

5.6.4.3 Professional Services Project Change Management

In the event of a project change request, the contractor shall provide clear justification for the change, cost and schedule impact, and proposed course of action. The contractor shall not proceed without COR approval.

5.6.5 Analysis and Requirements Services (ARS)

Analysis and Requirements Services shall be provided by the contractor for requirements development and management, which includes requirements elicitation, analysis, documentation, validation, and verification for business software and hardware projects. In addition, ARS shall provide decision support by analyzing potential solutions in the context of customer business requirements and constraints. Each request for ARS Services will be managed according to the definitions and processes defined in the following sections.

5.6.5.1 Requirements Oversight

ARS shall:

a. Develop and maintain, with COR oversight, the MSO Requirements Process, and related tools and templates.
b. Collect measurements to assist the Agency in demonstrating reduced costs and improved efficiencies in business and research operations.
c. Conduct requirements elicitation employing industry best practices to gather requirements from all relevant stakeholders to ensure that they reflect an accurate assessment of the customer's business needs.
d. Conduct requirements analysis distilling stakeholder requirements to the level of depth and detail necessary for full understanding and sufficient for system design.
e. Document requirements using a consistent and standardized method to improve communication and ensure buy-in from all stakeholders.

5.6.5.2 Requirements Validation

ARS shall:

a. Ensure all problems with the requirements documentation (understandability, completeness, ambiguities, standards, etc.) as identified by stakeholders are addressed and resolved to the group's satisfaction.
b. Verify that all requirements are implemented sufficiently to meet the customer's business need through requirements testing and analysis. The testing and analysis results are provided to all appropriate ITD Government and contractor personnel for consideration.

5.6.5.3 Requirements Management

ARS shall ensure that requirement changes throughout the course of the project are documented, analyzed, communicated and validated among all stakeholders, and a record of requirements changes is maintained as part of a project's record.

5.6.5.4 Decision Support

ARS shall provide information to assist decision-makers by analyzing potential solutions in the context of customer business requirements and constraints (e.g., time, budget, policy, regulations, etc.) and document the results. This documentation may take several forms dictated by a project's specific attributes and can include Business Case Analyses, Analyses of Alternatives, Cost Estimates or any combination thereof.

5.6.6 Software Development, Maintenance, and SharePoint Services

The contractor shall provide the capability to develop and maintain custom software solutions. New software development shall be fully documented and include the delivery of systems conforming to the operational environment and specified user requirements. Applications must be compatible with current components in the environment. Newly developed software shall not adversely affect system performance. The contractor shall demonstrate the operational capability of software prior to delivery and provide training, as necessary. Training may vary according to user levels/needs (e.g. end users, administrators, analysts, help desk support, management, etc.) The contractor shall conform to SDLC standards.

The contractor shall manage software sustainment. Software sustainment includes the processes, procedures, people, material, and information required to support, maintain, and operate the software aspects of a system. It includes sustaining engineering, data management, configuration management, training, survivability, environment, protection of critical program information, anti-tamper provisions, security, supportability and interoperability functions, COTS product management, and technology refresh. In addition, the contractor will develop and maintain baseline information about software modeled after Industry and Government best practices (e.g., application software, subcomponents, feature set, version, software provider, users, etc.).

The contractor shall perform software development upgrades and maintenance, including problem fixes, enhancements to existing capabilities, and build releases required to support changes. New releases of software must maintain previously provided functionality, while providing enhanced capabilities or systems corrections. Maintenance will include updates to the appropriate documentation. The contractor shall have the capability to customize software applications currently in use (see RFP Exhibit E).

The contractor shall provide SharePoint site design, development, implementation and administration services.

The contractor shall develop and implement secure web services and integrate with 3rd party Application Programming Interfaces (APIs).

The Government anticipates that development tools and languages will evolve over the life of this task order. The contractor shall design and develop using the most efficient and cost-effective methodologies available, ensuring that contractor staff have the training and skillsets to provide innovative solutions.

The contractor shall deliver software that is secure and accreditable. The contractor shall ensure security requirements are addressed in software design and development. The contractor shall conduct security scans, document vulnerabilities, correct vulnerabilities, and document the resolution or mitigation of vulnerabilities. The contractor shall support the Government's effort to accomplish accreditation by assessing the validity of vulnerabilities identified during accreditation testing, recommending, and after receiving Government approval, performing corrective actions to resolve or mitigate vulnerabilities.

5.6.7 Information Assurance and Network Defense

5.6.7.1 Compliance Directives

The contractor shall comply with DARPA's implementation of DoD Directives, Policy and Guidance on securing Information Systems.

5.6.7.2 ITD Security Services

The contractor shall interface with the Government to provide Defense-in-Depth by being an active and engaged partner in planning, designing, architecting and engineering security products and tools to meet IA and security initiatives as set forth by the Government. This role will receive tasks, requirements, policies and compliance directives as well as oversee the IA compliance, certification, accreditation, vulnerability assessments and the implementation of security for information systems across the task order functional areas. The contractor shall support the Government's lead for Incident Response Teams comprised of the applicable skill sets to respond to incidents when they occur. Overall the contractor shall ensure the Government's security requirements are met, complying with applicable DoD policies and providing Computer Network Defense Services to meet all security service and IA service requirements to protect the Government's Information Systems (IS) in accordance with DoD Directive O-8530.1 (Reference (f)).

As specified in the DoD Directive 8000.1 (Management of the Department of Defense Information Enterprise) (Reference (r)) and DoD Instruction 8510.01 (Risk Management Framework (RMF) for DoD Information Technology (IT) (Reference (e)), all automated systems and services shall meet fundamental security requirements and must be accredited by the Authorizing Official (AO) prior to processing classified or controlled unclassified information. All IT Services in this entire PWS shall be implemented with proper products, policies and procedures to ensure required system certification and accreditation in accordance with the applicable policies (Reference (e)).

The contractor shall coordinate Computer Network Defense services with the Government. In accordance with Government direction, the contractor shall support the application, implementation and execution of Computer Network Defense (CND) Services actions. The requirements of the CND Services are detailed in CJCSI 6510.01F, "Information Assurance (IA) and Computer Network Defense (CND)" (Reference (j)).

The contractor shall provide specific security services for the Government's
Information Systems (IS), Information Systems Domains (Communities of Interest), and Information Content (at rest, in use and in transit) that will include at a minimum, the following or equivalents:

a. Network boundary/perimeter protection, including firewalls, intrusion detection systems (IDSs) and Virtual Private Networks (VPNs).
b. Security monitoring and response
c. Incident Management, including emergency response and forensic analysis (SLO 4.1)
d. Vulnerability assessment and penetration testing and analysis of computers and networks
e. Anti-Virus and content filtering Services
f. Information Security Risk Assessments
g. Facilitate security information sharing and workflow across traditional organizational and functional lines
h. 24x7 Security Operation Services – The contractor shall provide support personnel for general Security Operation Services and to properly address or escalate an event, if necessary. This may include, but is not limited to, event analysis and resolution, calling in additional support personnel and alerting or escalating the event to the Government.
i. Monitoring and analysis of threats to the network infrastructure, and detection and rapid response commensurate with the threat's potential harm or damage to the Government's IT systems
j. An expert level of proficiency in tools, techniques and counter- measures in network vulnerabilities
k. Assistance in the development and maintenance of security policies and procedures
l. Assurance that policies and procedures are implemented and enforced, through both manual and automated controls
m. Management status reports and escalations on all security operation requests and problems
n. Participation in the remediation of audit findings
o. Implement procedures and metrics for security operations as specified by the Government
p. Implementation of automated tools for security operations

Due to the dynamic nature of IT-based attacks, significant advances will be expected in CND tools and practices over the life of this task order. The contractor shall be expected to continue to offer best-of-breed defense products and services, and employ industry best practices; therefore, the requirements listed above shall be considered as a baseline.

5.6.7.3 Information Defense (ID) Services

The contractor shall provide proactive cyber security services to monitor, detect, mitigate, and counter internal and external cyber threats posed to DARPA data and personnel. The contractor shall perform information threat analysis and conduct intelligence and profiling for DARPA information systems through passive and active monitoring, data sharing and collaboration, and advanced technical analysis. Information Defense services shall include:

a. Detection and mitigation of threats to DARPA information systems
b. Investigative and organic Cyber Intelligence (CI) activities
c. Malware analysis
d. Monitoring, via active and passive activities, of cyber threats to the DARPA information infrastructure
e. Advanced technical expertise and analysis of security incidents

f. Vulnerability assessments within the DARPA facility
g. Assessments of DARPA systems and networks, identifying deviations from acceptable configurations, DOD or DARPA policies
h. Authorized penetration testing of DARPA assets/networks
i. Coordination and sharing of information regarding cyber threats between DARPA staff, US Government Agencies, and, with Government approval, other contractors.
j. Recommendations for improved and innovative solutions and methodologies for detecting and mitigating cyber threats.

The contractor shall perform the following Information Defense activities:

a. E-Mail Analysis – A review of reported emails, tracking the following information to determine if it is indicative of a larger attack initiative:
    - E-mail origin
    - Delivery vectors
    - Payload usage
    - Social engineering patterns
    - Timing
    - Recipients
    - Crafting methodology
    - Any other perceived patterns that could potentially provide information for identifying trends of malicious activity
b. Malware Analysis – A review of detected or reported malware to garner information including: command and control information, attribution, detection characteristics, and capabilities. Specific data captured shall include: MD5/SHA1 hash, date/time of collection, source, and attributes collected. This data will be retained for trending and future analysis
c. Threat Profiling – The contractor shall monitor sensors and other data collection toolsets on DARPA networks. Data collected will include passive DNS collection, network flows, and a malicious code database.
d. Incident Response Support – The contractor shall provide advanced technical analysis during and after security incidents.
e. Cyber Threat Analysis and Coordination – The contractor shall, with proper Government oversight, coordinate, communicate, and collaborate with external Government entities to provide an independent assessment of the current information threat landscape and report and recommend appropriate defensive measures.

The ID function is currently staffed with three full-time equivalent (FTE) personnel.

NOTE: NO ANALYSIS WILL BE CONDUCTED ON WORKSTATIONS CONNECTED TO PRODUCTION NETWORKS.

5.6.7.4 Information Assurance (IA) Compliance

The Operation Services team members shall be responsible for ensuring that all workstations, servers, applications and services within the DARPA enclaves meet IA compliance criteria. This shall include applying all Government-directed IA mandates such as INFOCONs (Information Operations Conditions), Security Technical Implementation Guides (STIGs) (Reference (k)) and other Vulnerability Announcements. Implementation of IA mandates shall be in accordance with

Government-specified timeframes and SLOs. The contractor shall ensure that information systems/software remain compliant with all STIGs, and participate in quarterly reviews of STIG compliance conducted by the Government. Additionally, the contractor must support the NIST Security Automation Protocol (S-CAP which "automates" compliance reporting of the STIGs, when it is released. The contractor shall also be responsible for ensuring that the Government infrastructure meets the requirements for certification and accreditation in accordance with DoD policy (Reference (e)). The contractor shall maintain the state of all information systems/applications to ensure full compliance with Command Cyber Readiness Inspections checklists and in accordance with a Level-II Computer Network Defense Service Provider (CNDSP). To support Government oversight, the contractor shall make available, near real-time, data feeds, to include access to operating systems and networks, databases, access logs, Intrusion Defense Systems, and network tools.

When implementing updates, patches, service packs and hot fixes the contractor shall use tools that are, when possible, automated and transparent to the end-user and completed by DoD mandated deadlines. Such tools may include, but are not limited to, anti-virus programs and firewalls. The contractor shall verify compliance and ultimate mitigation of the vulnerability by using the DoD preferred and approved vulnerability scanner(s).

The Security Services Manager shall support the Information Systems Security Officer (ISSO) to coordinate application, implementation and execution of Computer Network Defense Services, IA policy, C&A, audits, mitigation recommendations, etc.

5.6.7.5 Public Key Infrastructure (PKI) Integration

The contractor shall provide continuous support, maintenance, integration and management of the DARPA Public Key Infrastructure (PKI) services, in compliance with DARPA implementation of DoD directives, specifically DoD Directive 8520.2 (Reference (d)). The primary medium assurance PKI credentials will be the CAC, a smart card, with certificates issued by the DoD. All PKI-enabled applications in DARPA must be compatible with the DoD PKI, and only DARPA-authorized certification authorities may issue certificates.

The DARPA PKI Service shall include directory services support, registration, interface to related Government systems, hosting of PKI-enabled servers, and required key management services as well as PKI solutions for e-mail, web applications, file transfer directory authentication, and VPN. At contract award the Government will provide the contractor with the DoD PKI user profiles as Government Furnished Information (GFI) to be implemented by the contractor. Certification Authority (CA) functions will be performed by the Government. Certificate requests shall be performed by the contractor. The contractor shall perform PKI management functions, including user registration. Additionally the contractor shall support the following:

a. The contractor shall use only DoD-compliant PKI-enabled servers where applicable
b. The contractor shall provide digital signature capability for all electronic mail services implemented, by utilizing the DoD-compliant digital signature certificates residing on the DoD-provided CAC smart card
c. The contractor shall register all users' PKI certifications. This shall include registration of identity and e-mail certificates (signature and confidentiality) as required.

d. The contractor shall provide user training for DoD PKI certificate use
e. The contractor shall register servers and install server certificates for PKI- enabled applications. DoD-compatible PKI certificates shall be used for client-server identification and authentication for all web servers on unclassified Government networks

5.6.7.6 Sensitive Information Support (Non-Classified)

Under current Federal guidelines, all officially held information is considered sensitive to some degree and must be protected by the contractor in accordance with the Privacy Act of 1974 (Reference (v)) and DoD 5400.11-R (Reference (w)) and as specified in the applicable IT Security plans, such as DoD Manual 5200.01 (Reference (h)), DoD Directive 5015.02-STD (Reference (b)), and other DoD directives, policy, and guidance as specified in the task order requirements and regulations covering the following:

a. Privacy Act Information
b. Proprietary information of partner and task order companies to DARPA
c. Information protected by International Traffic in Arms Regulation (ITAR)
d. Technology restricted from foreign dissemination
e. DARPA Proprietary and administrative communications, which includes senior Government officials, procurement and budget data, EEO, labor relations, legal actions, disciplinary actions, complaints, etc.
f. Freedom of Information Act (FOIA) and Personally Identifiable Information (PII)

The contractor shall perform internal assessments based on Government policies to determine position sensitivity and management controls necessary to prevent individuals from bypassing controls and processes, such as individual accountability requirements, separation of duties, access controls and limitations on processing privileges. These position sensitivity assessments shall be forwarded to DARPA designated personnel for a determination of personnel suitability and requirements for individuals assigned to these positions. Periodic re-evaluations of positions and suitability requirements shall be necessary during the life of the task order as positions and assignments change.

5.6.7.7 Sensitive Information Support (Classified)

DARPA handles data at all security levels. Occasionally, data contamination, or "spillage," occurs. A spillage is a security incident that results in the transfer of classified information to systems that are not approved to house or process that classification of data. In the event of a possible spillage of classified information onto the unclassified network, the contractor shall follow DARPA procedures and, to the extent possible, isolate and protect the classified information from unauthorized disclosure and from being spread further, while maintaining continuity of operations to the extent possible. Consideration should be given to law enforcement implications and preservation of evidence. The appropriate procedures for sanitizing or remediating the effects of a spill may include:

a. Using approved software to delete the spilled information.
b. Re-labeling the media containing the spilled information to the appropriate classification/category and transferring the media into an appropriate environment.
c. Removing the classified information from the media by Government-approved technical means to render the information unrecoverable.

d. Erasing and sanitizing the media.
e. Forfeiting the media which often includes backup tapes.

The contractor shall work with the DARPA SID and other organizations, per Government direction, to investigate, remediate, and take appropriate action in accordance with DoD 5220.22-M (Reference (i)), and DARPA's implementation of the DoD policy.

5.6.7.8 Privacy and Security Safeguards

The contractor shall not publish or disclose in any manner, without written consent of the Government, the details of any security safeguards designed, developed, or implemented by the contractor under this task order. When working with outside vendors, after having received Government written consent, the contractor must ensure that non-disclosure agreements are in place, before any security safeguard information can be shared. These restrictions are applicable to the contractor's off-site corporate offices as well. The contractor shall develop procedures to ensure that IT resources leaving the DARPA enclave, such as items being removed for repair, replacement or upgrade, are cleared of all Government data and sensitive application software by a technique approved by the Government. Damaged IT storage media shall be degaussed or destroyed in accordance with the approved DoD and DARPA security procedures, and ASD Memo, "Disposition of Unclassified DoD Computer Hard Drives Memorandum" (Reference (x)).

The Government will carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, availability and non- repudiation of Government data. The contractor shall provide the Government access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, system databases and personnel to facilitate the audits and inspections. The Government will conduct an audit on a periodic event-driven basis of the contractor's security management processes and procedures. These audits will include mock Command Cyber Readiness Inspections (CCRI) to ensure that the contractor has maintained full compliance.

5.6.7.9 Certification and Accreditation (C&A)

The contractor is responsible for maintaining and delivering systems that can be certified and accredited in accordance with DoD security requirements and processes defined in the Risk Management Framework (Reference (e)).

The contractor shall assist the Government in successfully completing system Certification and Accreditation (C&A), Information Support Plan (ISP) support and services including conducting initial certification tasks and periodic review of security configurations. The contractor shall review policy and procedure changes that have occurred since the system was last certified and accredited and recommend appropriate actions to address any deltas. The contractor shall assist the Government with the Risk Management Framework Implementation Plan, assignment of Information Assurance Controls, and completion of required security artifacts. The contractor shall assist the Government with risk and security-related documents such as a:

a. Risk assessment
b. Privacy impact assessment
c. System interconnection agreements
d. Contingency plan
e. Security configurations

f. Configuration management plan
g. Incident response plan
h. Continuous monitoring strategy.

The contractor shall also assist the Government in developing the following documents:

(A) Security Authorization Report (SAR):

a. Prepared by the security control assessor
b. Provides the results of assessing the implementation of the security controls identified in the security plan to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the specified security requirements
c. Contains a list of recommended corrective actions for any weaknesses or deficiencies identified in the security controls.

(B) Plan of Actions and Milestones (POA&M) (as required)

a. Prepared by the Information Security Officer (ISO) or common control provider
b. Describes the specific measures planned:
    i. to correct weaknesses or deficiencies noted in the security controls during the assessment; and
    ii. to address known vulnerabilities in the information system.

(C) Authorization Decision Document (ATO, IATT)

a. Transmits the final security authorization decision from the Authorizing Official (AO) to the information system owner or common control provider and other key organizational officials, as appropriate
b. Contains the following information:
    i. Authorization decision;
    ii. Terms and conditions for the authorization;
    iii. Authorization termination date; and
    iv. Risk executive (function) input (if provided).

(D) Supporting Documentation, including the Risk assessment report and all other artifacts specifically required for security control compliance.

5.7 Task Order Transition Services

5.7.1 Transition-In Services

The contractor shall be responsible for executing its transition plan (Attachment 7) to support the migration from the "as is" Government infrastructure at task order award to the contractor implemented Government infrastructure that will be certified and accredited in accordance with DoD Security Requirements. In order to provide continuity of unclassified ITD information technology services and support, the contractor shall assume full responsibility for all of the requirements in the PWS at the beginning of the Basic period of performance.

5.7.2 Transition-Out Services (Option – exercised one time only)

The contractor shall perform all activities in the subparagraphs to follow, including transition-out planning and reporting, and if required by the Contracting Officer, shall be required to continue to provide services during the transition-in period of the follow-on contractor in accordance with FAR clause 52.237-3 Continuity of Services.

5.7.2.1 Data and Files

The contractor shall relinquish all files and documentation related to this task order, including the media it is stored on (including paper, tape, CD, etc.), to the Government or its designee.

5.7.2.2 Explicit and Tacit Knowledge

The contractor shall transition all explicit and tacit knowledge related to this task order to the Government or its designee. Specifically, all documentation related to this task order, including processes, plans, procedures and methods, etc., regardless of the source or technique used to acquire this knowledge, is the property of the Government or its designee. Additionally, all documentation must be maintained online.

5.8 Deliverables and Delivery Schedule

A complete list of deliverables is included below. All deliverables are to be provided to the COR.

5.8.1 Information Technology (IT) Services Reporting

The contractor shall provide all reports under this PWS to the COR through the Government-owned electronic documents records management system. The Government currently uses Microsoft SharePoint.

a. Service Level Objectives (SLO) Data Report

The data shall include service levels achieved for the reporting period.

Frequency: Monthly (due 10 working days after the end of the month)

b. Network Failure Report

The data shall include detailed failure analysis and corrective actions applied for all network events that lasted 15 minutes or more, including at a minimum the following:

i. Summary of network availability and problems encountered
ii. Detailed failure analysis and corrective actions applied for all network events that caused a service interruption, including at a minimum the following:

(1) Event description, including network impact
(2) Event date, time and duration
(3) Services affected
(4) Information on how the event was detected
(5) Corrective actions
(6) Root cause analysis
(7) Preventative actions taken
(8) Date and time Government directed personnel were notified

Frequency: Monthly, Quarterly, and as needed

c. Interoperability Test Plan
The data shall include a plan and procedures to minimize the possibility of interoperability problems during modification of existing configurations.

Frequency: As Needed per CM Case

d. Asset and Credit Report and Asset Management Database
The data shall include description of asset, location of asset, quantity of asset, serial number/bar code, date of report, fair market value, received date, life cycle duration, purchase order cost, purchase order number, purchase order description, and warranty information, if applicable.

Frequency: Near Real-Time and Monthly

e. Software Asset Inventory and License Report
The data shall include the list of all customer-facing software, deployed version, latest available version, and indication that the latest version is deployed--or software purchased off the catalog, include the customer's name, netbios name of the system, and office. Separately, the data shall include all software licenses and maintenance agreements, their end date, and an indication if the licensing and maintenance are up to date.

Frequency: Monthly

f. Individual Tech Office/Functional Area Asset Inventory Report
The data shall include assigned office, Government or contractor, onsite/offsite, name, item description, catalog item description, cost, quantity and if applicable, bar code.

Frequency: Near Real-Time

g. Configuration Management/Diagram Reports
The documentation shall provide a systems architecture view of the Government network in the contractor's standard format. The data shall include a full description of all external interface points, to include DoD compliant technologies, protocols, and peering arrangements for external connectivity. It shall include physical and logical connectivity, and how interoperability is achieved at the interfaces. The architecture shall detail Government network hosting of current systems. Data shall include graphic architecture designs and cabling diagrams, at least to the building level.

Frequency: On-line, updated as necessary

h. Disaster Recovery Plan
The contractor shall provide and maintain a Disaster Recovery Plan and related Standard Operating Procedure with verification and test frequency.

Frequency: Quarterly

i. Continuity of Operations Plan (COOP)
The contractor shall participate in discussions and provide written input for creation and maintenance of a Continuity of Operations Plan, if required.

Frequency: As required

j. Information Feeds for Government Oversight
The data shall include an historical summary and management reports detailing Network Management System (NMS) functions.

Frequency: Near Real-Time

k. Weekly Activity Report (WAR)
The contractor shall generate two Weekly Activity Reports, the MSO WAR and the ITD WAR. In the MSO WAR, the contractor shall report current status of all on-going projects. In the ITD WAR, the contractor shall, at a minimum, summarize weekly Help Desk transactions (ticket types, file restoration results), asset management (counts and variances), configuration control, and other Government relations activities (User outreach, training, and survey results). The MSO WAR shall also provide a brief description of any Information System Security Officer (ISSO) Functions, system anomalies or unscheduled downtimes that occurred during the week. The contractor shall also prepare and present the status of other facets of the task order as specified by the Government.

Frequency: Weekly

l. Network Trend Analysis
The data shall include an analysis of network bandwidth and infrastructure resource utilization based on trends and observed growth patterns.

Frequency: Near real-time

m. Program Management Plan (PMP)
The contractor shall generate and maintain a program management plan, which will provide the means for managing and administering the services provided in this PWS. This plan shall include standard operating procedures, processes and methods, and security features as they apply to performance of the entire PWS. This plan shall also include the contractor's initial assessment of the requirements in the PWS, and address how the contractor will ensure ongoing compliance with this requirement.

Frequency: On line, updated as required

n. Organizational Chart
The contractor shall maintain a hierarchical staffing chart with position titles and names.

Frequency: On line, updated as changes occur.

o. IT Services Functional Area Financial Reporting
The contractor shall provide financial reports for the previous 12 month period for all cost elements, by technical office and functional area, under the task order in a Government approved format in near real-time, where appropriate as determined by the Government. Financial reports shall include reporting current month expenditures by element, technical office and functional area, and expenditure totals for each. Financial reports shall be supplemented with invoices

submitted in accordance with this task order.

Frequency: Monthly

p. Monthly Cost Status Reviews

The contractor shall provide monthly briefings at the DARPA facility that provide overviews of financial and task order status of the IT Services task orders for the previous 12 month period, broken out by technical office and functional area in a Government approved briefing package format. This brief shall include, but is not limited to, Financial/Contractual Program Actions, Funding Issues, and Pending Actions. A cost trend by functional area shall be presented in graphical form.

q. Task Order Financial Summary Report

The report shall include the following data:

(1) Recap from Previous Month:

- Task Order Financial Summary
  - Estimated Task Order Value
  - Estimated Task Order Fee
  - Total Estimated Task Order Value
  - Expensed
  - Task Order Funding Inception to Date (ITD) Funded including Fee
  - ITD Expensed including Fee
  - Balance

(2) Task Order Expenditure Recap:

- Mod Number
  - Period
  - Funding Allocation
  - Expenditure
  - Fee Earned
  - Balance

(3) CY Expenditure Elements:

- Period
- Invoice Number
- By CLIN
- Total

(4) COTS Catalog Activity:

- Current Period COTS
- Adjustments
- Current Expenditures Total
- YTD COTS Expense (Task Order and Fiscal)
- ITD only COTS Expense

(5) COTS Activity by Office:

- Office
- Current Period

- YTD (Task Order and Fiscal)
- Graphic to reflect
  - Current Period by Office
  - YTD Trends by Office

Frequency: Monthly

r. SLO Monitoring/Trending Report
The contractor shall establish and maintain a Service Level Objective monitoring chart to be used to help track and report achievements and trends against Service Level Objectives. The chart shall show whether each agreed Service Level Objective has been met or missed during each of the previous 12 months.

Frequency: Monthly

s. Operations Status Report
The contractor shall provide a network status report, including work conducted overnight (from 7 p.m. to 7 a.m.) backup success or failures, status of the following network services, file services, email, Internet, VPN, SAN replication, etc. Additionally, the contractor shall provide the status of any service degradation or outages which have occurred after core hours.

Frequency: Daily

t. Account Inactivity Report
The contractor shall provide an Account Inactivity Report that identifies all User Accounts on the DMSS network that have not been accessed in the past 30, 60, and 90 days.

Frequency: Monthly

u. Plan of Action & Milestones (POA&M)
The contractor shall provide a task order-level Plan of Action and Milestones (POA&M) covering the duration of the current task order year with updates provided quarterly at a minimum.

Frequency: Quarterly

v. Software Development Plan
The contractor shall provide a Software Development Plan to identify and describe the policies and methods employed during the life cycle management of all applications for the task order. It describes the contractor's formal Software Lifecycle approach for development of information technology (IT) applications utilized by DARPA personnel.

Frequency: Annually

w. Daily After-Hours Help Desk Ticket Summary
The contractor shall provide a Daily After-Hours Help Desk Ticket Summary that identifies all Help Desk System Tickets received during previous days' non-core hours. At a minimum, it will cover the following:

a. Help Desk ticket number
b. User name and DARPA Office designator
c. Date/Time of ticket
d. Status as of 7am
e. One line summary of issue

Frequency: Daily

x. Ad-Hoc Management Reports
The contractor shall provide reports for all aspects of performance under the Task Order, as requested by the COR. At a minimum, they will cover the following:

- Financial, including budget
- Issues to be resolved
- Government services
- Program-related
- Work plans
- Modernization recommendations, plans, and progress
- Security issues, status and progress
- Quality control
- Automated Resource Management System and Inventories
- Human resources

Frequency: As Requested by the Government

5.8.2 Information Assurance (IA) Services Reporting

a. Security Incident Report
The data shall include any security incidents, regardless of level, to include computer, network, server, configuration changes, INFOCON status, and intrusion detection system (IDS) reaction alert status.

Frequency: Upon Incident

b. Certification and Accreditation (C&A) Documentation
The data shall include the following:

a. CONOPS (Concept of Operations)
b. Automated Information System Security Plan (AISSP)
c. Risk Assessments
d. Vulnerability Assessments
e. Risk Mitigation Plans

Frequency: As required

c. Security Status Report
The data shall include real time or near real time data feeds (i.e., dashboards) supporting Government oversight of security functions.

Frequency: Near Real-Time

d. Security Management Practices and Procedures
The documents shall include security procedures describing how IA mechanisms will be operated to provide the security services specified in the PWS.

Frequency: Quarterly

e. Information Technology (IT) Security Plan
The contractor shall provide an Information Technology Security Plan for sensitive information Systems.

Frequency: As required

f. Sensitive Information Systems: Position Assessments
The contractor shall provide position assessments based on Government policies regarding position sensitivity and management controls necessary to prevent individuals from bypassing controls and processes.

Frequency: Quarterly

g. Security Architecture
The data shall include architecture diagrams that depict how information is transferred through defense in depth boundaries 1 through 4. Diagrams shall include the proposed employment of all major network components (at a minimum firewalls, intrusion detection systems, servers, routers, switches, load- balancers, and data path) which play a significant role in network operation, management, and security. Diagrams shall also indicate location of alternate paths and backup equipment. This includes information sources, supporting paths and capacities, any unique manipulation of data in transit, points of termination and placement of all proposed security components. Diagrams shall address unclassified architectures, and also any unique architectural differences associated with different types of locations.

Frequency: As Requested

h. Security Architecture Updates
The contractor shall propose updated and revised security architecture designs for Government review and approval to accommodate changing requirements, emerging technologies, and the results of vulnerability assessments.

Frequency: As required

i. Risk Assessment Plan
The contractor shall provide and maintain a Risk Assessment Plan.

Frequency: On line (at least monthly)

j. Risk Management Framework (RMF) Package Support
The contractor shall assist the Government with the RMF process, including all required documentation.

Frequency: As required

k. Vulnerability Announcements/Patch Report and Communications Tasking Order (CTO) Items
The data shall include a summary of Vulnerability Announcement mitigations/patch activity for management review. Information will be maintained online.

Frequency: Near real-time

l. IDS-Detected Attacks
The data shall include a summary of each intrusion detection system (IDS) alert, its detection, identification, containment, and resolution.

Frequency: Monthly

m. Signature/Profile Configuration Status
The data shall include current status of all signature/profile configurations.

Frequency: Monthly

n. Signature/Profile Maintenance and other Scheduled Outages
The data shall include statistics for all signature/profile maintenance and other IA related scheduled outages that occurred during the reporting period.

Frequency: Monthly

o. Signatures, Profiles and Alert Mechanism Testing Results
The data shall contain results of periodic testing of signatures, profiles and alert mechanisms.

Frequency: Monthly

p. Log Trending and Analysis
The data shall include a summary of anomaly detection and traffic analysis based on system logs.

Frequency: Monthly

q. Current Firewall Configuration
The data shall include but is not limited to the current firewall rule sets, firmware version, and security configuration.

Frequency: Monthly

r. Open and Closed Ports and Protocols
The data shall include but is not limited to what ports are open and closed and what protocols are allowed and disallowed internally and externally from the networks.

Frequency: Monthly

s. After-Hours Administration Logins and Activities
The data shall include any administrative logins and the administrator's activity outside of the core hours.

Frequency: Daily

5.8.3 Catalog Services Reporting
All reports should be searchable and sortable at the agency, office and individual levels.

a. Government Reviews of Services
The contractor shall provide quarterly status briefings of the services listed in the service portfolio and service catalog, to the Government.

Frequency: Quarterly

b. Order Status Report
The data shall include ordering office, order number, order date, order status, back order date, ordered amount due, date order created, order created by User ID, date order last modified, number of ordered products, ordered product, product number, quantity, order product status and unfilled orders status, quantity shipped, date shipped, quantity installed, and order price.

Frequency: Near Real-Time

c. Catalog Expenditure Report
The report shall be sorted by the following variables: Office, Fiscal Year, Expenditure Status (Committed, Pending Approval, and Open). Data shall include ordering office, Fiscal Year, current funding level, order date, order number, order created by User ID, order item, order status, cost, total by expenditure status, funds remaining.

Frequency: Near Real-Time

d. Pending Order Approval Report
The data shall include order number, order created by User ID, order office, order submitted date, order status, order Fiscal Year. Users shall be able to access any individual order via a link directly from the report.

Frequency: Near Real-Time

e. Pending Catalog Item Entry Approval Report
The data shall include Item ID, Item Name, cost, associated order number.

Frequency: Near Real-Time

f. Catalog Ad-Hoc Reports
The contractor shall provide continuous support in order for ITD to self-generate ad-hoc reports of information contained in the catalog as requested by the Government.

5.8.4 IT Governance Reporting

a. Fielding and Implementation Plan
The contractor shall generate an implementation plan, which will provide the means for coordinating system, product, and service rollouts and tests with the Government. This plan shall reflect the actions identified in the Risk Assessment, C&A, and Security CONOPS (including Disaster Recovery Plan), and Interoperability Test Plan.

Frequency: One-Time at task order Start and updated as appropriate

b. contractor Configuration Management Plan (CMP)
The data shall include organizational structure, roles, responsibilities, policies, and methods employed for configuration management.

Frequency: Quarterly

c. Mobile Device Usage Report
The contractor shall report all mobile device usage minutes.

Frequency: Monthly

d. Daily Telephone Change Report
The contractor shall report all desk phone number and location changes.

Frequency: Daily

e. Weekly Telephone Ticket Requests
The contractor shall report the quantity of actions taken (including responses to customer requests).

Frequency: Weekly (Mondays for the previous week)

f. Configuration Change Request
The report shall include, at a minimum:

a. Type of Request
b. Priority Level
c. Name/Organization of Requestor
d. Explanation of Change
e. Justification of Change
f. Impact of Change
g. Security Concerns, Known Risks

h. Schedule

Frequency: As Requested

g. Technical Review and Interoperability Test Plan
The report shall include, at a minimum:

a. Background
b. Executive Summary of Testing Done
c. Test Plan and Results Matrix
d. Test Summary

Frequency: Per Configuration Management (CM) Case

h. Contractor Self-Assessment
The contractor shall provide a quarterly self-assessment report in accordance with the Award Fee Plan.

Frequency: Quarterly

i. Legacy Applications–Operational Level Agreements (OLAs)
The data shall include all OLAs in-place between the contractor and the Government.

Frequency: At Task Order Start and Updated As Needed

j. Application Management Plan

The contractor shall provide an Application Management Plan to identify and describe the policies and methods employed to ensure the performance, security, stability, reliability, consistency, and availability of Custom Developed Software, COTS and Third Party Software, Network and Configuration Updates, and Application End of Life policies.

Frequency: Annually

k. Technology Refresh Deployment Methodology and Schedule

The data shall include the technology refresh deployment approach, timing, scheduled downtime and impact to the production environment for each planned technology refresh (PWS ref: Release and Deployment Management).

Frequency: As Needed

5.8.5 Transition Services Reporting

a. Task Order Transition-in Plan
The contractor shall execute to and update, if necessary, its task order transition-in plan (Attachment 7), which will provide the means for managing and administering the effective and orderly transition of services from the incumbent contractor to include processes and procedures.

Frequency: Update within 10 days of task order start, if necessary.

b. Task Order Transition-out Plan
The contractor shall generate, execute, and maintain a task order transition-out plan, which will provide the means for managing and administering an effective and orderly transition of services to a follow-on contractor or any party designated by the Government.

Frequency: As directed by the Government prior to Task Order End

5.9 Government Furnished Space, and Information (GFS and GFI):

5.9.1 Government Furnished Spaces (GFS)

The Government will provide Government-furnished space on-site for the areas identified below. The areas identified below will be equipped with furniture, equipment, IT equipment, telephone services, office supplies, etc. needed for the performance of this task order.

a. Work space and warehousing,
b. On-site lab and Help Desk support,
c. Computer room, office spaces and Network and Security Operations Center (NSOC).,
d. Office space

5.9.2 Government Furnished Information (GFI)
The Government will furnish required and available Government information as needed and as available when there is a jointly agreed upon (Government and contractor) task order performance need.

5.10 Place of Performance:
Work will be performed at the Government designated site(s), approved contractor facilities, and or Facilities as described in this PWS. In addition, there may be occasional “limited” local or long distance travel (destinations and duration TBD) in support of performing the ITD mission.