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