Enterprise Infrastructure Solutions (EIS) Contract

Section C
Description / Specifications / Statement of Work

Issued by:
General Services Administration
Office of Information Technology Category
1800 F St NW
Washington, DC 20405

November 2023

Table of Contents

C.1 Background

The General Services Administration (GSA), Federal Acquisition Service, Integrated Technology Services (ITS), Network Services Program (NSP[1]) establishes and manages a range of acquisition programs to meet the needs of federal agencies for telecommunications, networking services and associated support.

This Request for Proposals (RFP) describes the government's requirements for the Enterprise Infrastructure Solutions (EIS) contract.

C.1.1 EIS Goals

The EIS contract is intended to meet the program goals for:

- Service Continuity.
- Highly Competitive Prices.
- High-Quality Service.
- Full Service Vendors.
- Operations Support.
- Transition Assistance and Support.

The overarching goal for EIS is to make the resulting contracts as flexible and agile as possible to meet and satisfy the widely differing requirements of the federal agencies both now and for the next decade and beyond.

C.1.2 EIS Scope for Mandatory and Optional Services

The EIS mandatory services include the following:

• Virtual Private Network Service	Specified in Section C.2.1.1
• Ethernet Transport Service	Specified in Section C.2.1.2
• Voice	Specified in Section C.2.2.1 and C.2.2.2
• Managed Network Service	Specified in Section C.2.8.1

It should be noted that Access Arrangements (Section C.2.9) are included as a mandatory component and shall be priced. The contractor shall also provide Voice services to non-domestic locations as defined in Section J.1.2.

Any service included in Section C.1.8.1 that is not listed above is considered optional.

[1] See http://www.gsa.gov/portal/category/22151 for background

C.1.3 Minimum Requirements for Geographic Coverage

The contractor shall provide EIS services on a global basis. Geographic coverage for domestic and non-domestic locations is specified in Section J.1. Domestic locations are further divided into CONUS and OCONUS.

CONUS Geographic requirements are defined by a set of domestic cities, based on the Core Based Statistical Areas (CBSAs) as defined in OMB Bulletin No. 13-01, dated February 28, 2013. The minimum mandatory geographic coverage area includes any 25 of the top 100 CBSAs provided by the government in Section J.1. The CBSAs listed are ranked in descending order of government bandwidth usage. It should be noted that there are over 900 CBSAs in the U.S. requiring services.

Notwithstanding the minimum requirements, the contractor is encouraged to propose the mandatory and optional services within any CBSA, OCONUS or non-domestic locations, whether included in Section J.1 or not, as long as the offer includes at least 25 of the top 100 CBSAs listed in Section J.1.

The contractor shall provide the mandatory services to all government locations within each of its selected CBSAs.

C.1.4 Task Orders

The government will order services in accordance with FAR Subpart 16.505. Agencies will conduct fair opportunity and award task orders (TOs) in accordance with the aforementioned subpart and the terms and conditions of this contract. For more detail, see Section G.3.

C.1.5 Authorized Users

This contract is for the use of all federal agencies, authorized federal contractors, agency-sponsored universities and laboratories, other organizations as defined in Section H.3, and, when authorized by law or regulation, state, local, and tribal governments.

C.1.6 Upgrades and Enhancements

The government recognizes that telecommunications technologies and services are rapidly evolving. Accordingly, the government anticipates that services and solutions available under this contract will be increased, enhanced, and upgraded as these improvements become available to commercial customers.

As the virtualization of infrastructure continues from computing to networking, the government is interested in the deployment roll-out of Network Function Virtualization and Software Defined Network (NFV/SDN) in the contractor's backbone wide area network (WAN), because the SDN supports quick provisioning and easy management.

Network function virtualization (NFV) is the virtualization of network equipment functions, which typically run on dedicated appliances, to now run on industry-standard servers, switches and storage devices with the aim of lowering costs, improving efficiency and increasing agility, via hypervisor technologies. Standards are being created by the European Telecommunications Standards Institute (ETSI), including major telecom equipment vendors and communications service providers (CSPs), with involvement by the Open Networking Foundation.

Software Defined Networking (SDN) is an approach to networking in which control is decoupled from the physical infrastructure, allowing network administrators to support a network fabric across multi-vendor equipment. The SDN decouples network control and forwarding functions, enabling network control to become directly programmable and the underlying infrastructure to be abstracted from applications and network services, by supporting the following capabilities:

1. Transport independence by disaggregating the service from the physical network.
2. Security (encryption and device authentication) at the routing level.
3. Allow network segmentation with different segments having different encryption schemes.
4. Centralized policy and control of all the devices across the network.
5. Allow Layer 4-7 services (to be advertised) on demand.

This will allow network managers, both agency and service providers, to configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs/codes (APIs), which they can write themselves because the programs/codes do not depend on proprietary software.

C.1.7 Organization of this Statement of Work

Section C.2 provides the technical requirements addressed by this contract. Section C.1.8 describes the general requirements and the format for the specification of the individual service areas and services, which are contained in Sections C.2.1 through C.2.12. Section C.3 contains requirements for management of transition from another expiring GSA-administered contract to EIS. Section C.4 specifies the government’s requirements for Section 508 compliance that have been established to ensure access to information and services by government employees and citizens with disabilities.

C.1.8 General Requirements

C.1.8.1 Organization of EIS Services

EIS service areas and services are presented in the following table.

Service Area	Service
Data Service	VPNS Ethernet Transport Optical Wavelength Service Private Line SONET Dark Fiber Internet Protocol Service Broadband Internet Service
Voice Service	IP Voice Service Circuit Switched Voice Service Toll Free Service CSDS
Contact Center Service	Contact Center Service
Colocated Hosting Service	Data Center Service
Cloud Service	Infrastructure as a Service Platform as a Service Software as a Service Content Delivery Network Service
Wireless Service	Wireless Service
Commercial Satellite Service	Satellite Service

Service Area	Service
Managed Services	Managed Network Service Web Conferencing Service Unified Communications Service Managed Trusted Internet Protocol Service Managed Security Service Managed Mobility Service Audio conferencing Video Teleconferencing Intrusion Prevention Security Service Software Defined Wide Area Network Service
Access Arrangements	Access Arrangements
Service Related Equipment	Equipment
Service Related Labor	Labor
Cable and Wiring	Cable and Wiring

IT-related products and services listed in the table above may be acquired only if they are associated to an infrastructure or telecommunications solution acquired through EIS.

C.1.8.2 Service Locations

A Service Delivery Point (SDP) is the interface point at which a service is delivered by the contractor to the government or its designated agent. The SDP is the interface point for the physical or logical delivery of a service and the point at which performance parameters are measured to determine compliance with the contract.

C.1.8.3 Performance

Almost all EIS services have a specified standard set of common metrics or Key Performance Indicators (KPIs) to measure and report their performance. This standard set of KPI's measures the primary dimensions an agency needs in order to evaluate service effectiveness. The underlying KPI computations are service specific or context sensitive (as defined within each service) to reflect the broad range of service offerings and the EIS focus on delivery of end to end services. The seven standard KPIs used for most services as specified within this contract are defined below.

Standard KPIs:

No.	KPI	Abbreviation
1	Availability (Service)	Av(S)
2	Time to Restore	TTR
3	Grade of Service (Service)	GOS(S)
4	Latency (Service)	Latency(S)
5	Jitter	Jitter
6	Event Notification	EN
7	Response Time	RT

For certain services, when required by agency customers, two service levels are specified. Routine service levels apply for most government applications. Critical service levels are defined for agency applications requiring higher levels of availability, performance, or restoral criteria. Critical service levels will be sought in the TO fair opportunity process. The parameters specified in the service descriptions shall apply to all domestic (both CONUS and OCONUS) services. Performance parameters for non-domestic services are specified in Section C.1.8.5. In addition, the performance provided shall always be at a level not less than what is generally available commercially, at no additional cost to the government. Thus, if the available commercial performance parameter is more demanding than the minimum acceptable level specified in this contract, the available commercial performance parameter shall take precedence.

As standards evolve, the contractor may propose and provide alternatives to the government that meet or exceed the standards listed per specific service.

C.1.8.4 Conformity to Standards

Throughout Section C, references are made to standards (including interim standards, Internet Engineering Task Force (IETF) Requests for Comments (RFCs), or de-facto standards) as they existed at the time of contract award. If a standard is defined by a specific version and/or date, then that specific version of the standard shall be implemented. Otherwise, compliance with the latest versions of these standards is expected. American national standards shall supersede international standards for services to be provided to on-net users located in the U.S. Where multiple standards are cited, the order of precedence shall be the industry forum specification, followed by ANSI, followed by iconectiv, and followed by ITU-TSS, unless otherwise specified.

C.1.8.5 Non-Domestic

Coverage includes delivery of service from domestic SDPs to non-domestic SDPs, from non-domestic SDPs to domestic SDPs, and from non-domestic SDPs to non-domestic SDPs. The following requirements for the numbering plan, features, performance, interfaces, security, and management and operations considerations that are applicable to the non-domestic services shall supersede the corresponding requirements specified for the domestic services:

1. **Numbering Plan.** The numbering plan for non-domestic locations shall conform to country-specific numbering plans.
2. **Features.** All features identified as mandatory in each service description shall be provided to non-domestic SDPs in the areas involved.
3. **Dial-In.** The contractor shall support country-specific non-domestic PSTN numbers and/or toll-free numbers, if commercially available, for dial-in access of services.
4. **Performance.** The KPIs in the performance metrics for each service between non-domestic SDPs or between domestic and non-domestic SDPs shall be compliant with the best commercial values or practices for those parameters within the non-domestic country and/or jurisdiction hosting the non-domestic SDPs.
5. **Interfaces.** When a service is delivered to an SDP at a non-domestic location, the UNI, e.g., interface type, payload data rate, protocol type, standard for the SDP shall comply with the country-specific interface standards when delivering service to the country-specific government equipment. However, if the government equipment conforms to a North American standard, then the UNI standard at the SDP shall comply with the North American standard where permitted by local law and regulations.

C.1.8.6 Interoperability

The contractor shall support interoperability for given service offerings so that a user of a service from one EIS contractor shall be able to communicate with users of services from other EIS contractors with equivalent performance. GSA recognizes that different levels of interoperability exist commercially, particularly in the area of data networking. Interoperability shall be made available for any service that is currently commercially offered by the contractor and is interoperable with the services of other EIS contractors. In addition, the contractor shall make available any future service interoperability at no additional cost to GSA when the contractor offers the interoperability for its commercially provided service.

Since near full interoperability is provided via the Public Switched Telephone Network (PSTN) for circuit switched services, the contractor shall support interoperability between voice services, circuit switched data service, and wireless services if offered. The contractor shall also support connectivity and interoperability for remote and mobile users as specified in the individual service descriptions.

C.1.8.7 System Security Requirements

Communications services under this contract will carry non-sensitive programmatic and administrative traffic, Controlled Unclassified Information (CUI) traffic, and higher levels of sensitive and/or classified traffic up to and including Top Secret/SCI that may be encrypted by agency users. Therefore, the contractor is required to provide basic security for all network services, as well as the network management systems and information systems and databases used to support those services. Such security shall include protecting all network services, information, contractor infrastructure, and information processing resources against threats, attacks, or failures of systems.

The contractor shall ensure that all services provided comply with all Federal Information Security Management Act (FISMA), DOD, and Intelligence Community requirements where applicable. The contractor shall submit a Risk Management Framework Plan describing its approach for security compliance for all services provided under EIS. This plan shall be submitted with the proposal in accordance with National Institute of Standards (NIST) Special Publication (SP) 800-37.

C.1.8.7.1 System Security Compliance Requirements

In providing EIS services, the contractor shall comply with all applicable federal and agency-specific IT security directives, standards, policies, and reporting requirements. The contractor shall comply with FISMA, DOD and Intelligence Community-associated guidance and directives to include all applicable Federal Information Processing Standards (FIPS), NIST SP 800 series guidelines (FIPS and NIST SPs available at: http://csrc.nist.gov/), agency-specific security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of government IT. In addition, the contractor shall comply with all service specific security requirements identified within Section C.2 Technical Requirements (e.g., Cloud Infrastructure as a Service (IaaS), or Managed Trusted Internet Protocol Services (MTIPS)).

Compliance references include, but are not limited to:

- Federal Information Security Management Act (FISMA) of 2002; (44 U.S.C. Section 301. Information security) available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
- Federal Information Security Modernization Act of 2014; (to amend Chapter 35 of 44 U.S.C.) available at https://www.congress.gov/113/bills/s2521/BILLS-113s2521es.pdf.
- Clinger-Cohen Act of 1996 (formerly known as the “Information Technology Management Reform Act of 1996”) available at: https://www.fismacenter.com/Clinger%20Cohen.pdf.
- Privacy Act of 1974 (5 U.S.C. § 552a).
- Homeland Security Presidential Directive (HSPD-12), “Policy for a Common Identification Standard for Federal Employees and contractors”, dated August 27, 2004; available at: http://www.idmanagement.gov/.
- Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources”, and Appendix III, “Security of Federal Automated Information Systems”, as amended; available at: http://www.whitehouse.gov/omb/circulars_a130_a130trans4/.
- OMB Memorandum M-04-04, “E-Authentication Guidance for Federal Agencies” (Available at: http://www.whitehouse.gov/omb/memoranda_2004).
- OMB Memorandum M-14-03. “Enhancing the Security of Federal Information and Information Systems” available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.
- FIPS PUB 199, “Standards for Security Categorization of Federal Information and Information Systems.” Dated February 2004.
- FIPS PUB 200, “Minimum Security Requirements for Federal Information and Information Systems.” Dated March 2006.
- FIPS PUB 140-2, “Security Requirements for Cryptographic Modules.” Dated May 2001.
- FIPS PUB 140-3, “Security Requirements for Cryptographic Modules.” Dated March 2019.
- NIST SP 800-18 Revision 1, “Guide for Developing Security Plans for Federal Information Systems.” Dated February 2006.
- NIST SP 800-30 Revision 1, “Guide for Conducting Risk Assessments.” Dated September 2012.
- NIST SP 800-34 Revision 1, “Contingency Planning Guide for Information Technology Systems.” Dated May 2010.

- NIST SP 800-37 Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.” Dated February 2010.
- NIST SP 800-40 Revision 3, “Guide to Enterprise Patch Management Technologies.” Dated July 2013.
- NIST SP 800-41 Revision 1, “Guidelines on Firewalls and Firewall Policy.” Dated September 2009.
- NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems.” Dated August 2002.
- NIST Special Publication 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations.” Dated April 2013.
- NIST Special Publication 800-53A, Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans.” Dated December 2014.
- NIST SP 800-58 “Security Considerations for Voice Over IP Systems.” Dated January 2005.
- NIST SP 800-60 Revision 1, “Guide for Mapping Types of Information and Information Systems to Security Categories.” Dated August 2008.
- NIST SP 800-61 Revision 2, “Computer Security Incident Handling Guide.” Dated August 2012.
- NIST SP 800-88 Revision 1, “Guidelines for Media Sanitization.” Dated December 2014.
- NIST SP 800-94 “Guide to Intrusion Detection and Prevention Systems.” Dated February 2007.
- NIST SP 800-128 “Guide for Security-Focused Configuration Management of Information Systems.” Dated August 2011.
- NIST SP 800-137 “Information Security Continuous Monitoring for Federal Information Systems and Organizations.” Dated September 2011.
- NIST SP 800-144 “Guidelines on Security and Privacy in Public Cloud Computing.” Dated December 2011.
- NIST SP 800-160 “Systems Security Engineering.” dated November 2016.
- NIST SP 800-161 “Supply Chain Risk Management Practices for Federal Information Systems and Organizations.” Dated April 2015.
- NIST SP 800-171, “Protecting Controlled Unclassified Information in the Nonfederal Information Systems and Organizations.” Dated June 2015.

- Committee on National Security Systems (CNSS) Policy No. 12, National Information Assurance Policy for Space Systems Used to Support National Security Missions. Dated 28 November 2012.
- Committee on National Security Systems (CNSS) Policy No. 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems. Dated 1 October 2012.
- Committee on National Security Systems Instruction (CNSSI) No. 1253, Security Categorization and Control Selection for National Security Systems. Dated March 2012.
- Committee on National Security Systems Instruction (CNSSI) No. 5000, “Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony.” Dated April 2007.
- Department of Defense Instruction (DODI) 8500.01 “Cybersecurity.” Dated 14 March 2014.
- DODI 8510.01 “Risk Management Framework (RMF) for DOD Information Technology (IT).” Dated 12 March 2014.
- Department of Defense (DOD) Cloud Computing Security Requirements Guide (SRG). Draft Dated 7 December 2014.
- ICD 503, “Intelligence Community Information Technology Systems Security: Risk Management, Certification and Accreditation.” Dated 15 September 2008.
- ICD 703, “Protection of Classified National Intelligence, Including Sensitive Compartmented Information.” Dated 21 June 2013.
- ICD 704, “Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information.” Dated 1 October 2008.
- ICD 705, “Sensitive Compartmented Information Facilities.” Dated 26 May 2010.
- ICD 731, “Supply Chain Risk Management.” Dated 7 December 2013.
- “IT Security Procedural Guide: External Information System Monitoring CIO-IT Security-19-101”
- Other agency-specific policies, directives and standards as identified at the TO level.

C.1.8.7.2 Security Compliance Requirements

FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems,” is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in eighteen security-related areas. Contractor systems supporting agencies must meet the minimum security requirements through the use of the security controls in accordance with NIST Special

Publication 800-53, Revision 4 (hereinafter described as NIST SP 800-53) “Recommended Security Controls for Federal Information Systems.”

To comply with the federal standard, the government has determined the security category of the information and information system in accordance with FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems,” to be established at a minimum of a Moderate Impact Level and baseline security controls must be established as identified in NIST SP 800-53 and other associated directives and guides identified and/or provided by each specific agency.

The government recognizes that these requirements are evolving and will make the necessary updates as the standards are formally implemented to reflect the changes.

If a Cloud solution is used (meeting the NIST definition of Cloud as stated in C.2.5) the security category of the information and information system will be established at a minimum of a Moderate Impact Level and the baseline security controls, applicable directives and guides as well as deliverables that must be adhered to are identified at www.FedRAMP.gov.

GSA will not be an EIS contractor FedRAMP sponsor at the contract level.

C.1.8.7.3 Security Assessment and Authorization (Security A&A)

In addition to the contractor’s Business Support System (BSS) requirements identified in Section G.5.6, the implementation of any contractor IT system that stores, transports or processes federal government data requires a formal approval process known as security A&A. NIST SP 800-37, Revision 1 (hereinafter listed as NIST SP 800-37) and agency-specific IT security procedural guidance, associated with managing enterprise risk, provides guidance for performing the security A&A process.

The contractor’s system must have the capability to provide a valid security A&A (when required by agency TO) prior to being placed into operation and processing government information for that agency. Agencies may require higher level certifications to be addressed at the TO level. Failure to obtain and maintain a valid assessment and authorization will be grounds for termination of a TO.

C.1.8.7.4 System Security Plan (SSP)

For delivery of services under a TO, the contractor shall comply with all security A&A requirements mandated by federal laws, directives and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The level of effort for the security assessment and authorization is based on the System’s NIST FIPS Publication 199 categorization. The SSP shall be completed in accordance with NIST Special Publication 800-18, Revision 1 (hereinafter listed as NIST SP 800-18) and other relevant guidelines. The SSP shall describe the contractor's approach for security compliance for all services provided under the EIS contract. The SSP shall also include, at a minimum, appendices and attachments specifically identified within the TO.

C.1.8.7.5 System Security Plan Deliverables

TOs will specifically identify the system security deliverables to be provided to an Ordering Contracting Officer (OCO), Information System Security Officer (ISSO), or Information System Security Manager (ISSM) initially, quarterly and on an annual basis, or when significant changes, as defined in NIST SP 800-37, occur to the system.

C.1.8.7.6 Additional Security Requirements

ID Number	Description
1	The deliverables identified in Section C.1.8.7.5 shall be labeled "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) or contractor selected designation per document sensitivity. External transmission/dissemination of CUI data to or from an agency computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2 & 140-3, "*Security requirements for Cryptographic Modules.*"
2	The government has the right to perform manual or automated audits, scans, reviews, or other inspections of the contractor's IT environment being used to provide or facilitate services for the government. In accordance with the FAR (see Section I, 52.239-1) the contractor shall be responsible for the following privacy and security safeguards: 1. The contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the contractor under this TO or otherwise provided by the government. *Exception - Disclosure to a Consumer Agency for purposes of security assessment and authorization verification.* 2. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, availability and confidentiality of any non-public government data collected and stored by the contractor, the contractor shall afford the government logical and physical access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods: • Authenticated and unauthenticated operating system/network vulnerability scans, • Authenticated and unauthenticated web application vulnerability scans, • Authenticated and unauthenticated database application vulnerability scans, and • Internal and external penetration tests. 3. Automated scans can be performed by government personnel, or agents acting on behalf of the government, using government operated equipment, and government specified tools. If the contractor chooses to run its own automated scans or audits, results from these scans may, at the government's discretion, be accepted in lieu of government performed vulnerability scans. In these cases, scanning tools and their

ID Number	Description
	configuration shall be approved by the government. In addition, the results of contractor-conducted scans shall be provided, in full, to the government.

C.1.8.7.7 Personnel Background Investigation Requirements

The contractor shall perform personnel security / suitability checking in accordance with FAR Part 52.204-9 (see Section I).

All contractor personnel with access to government information that is within the security A&A scope must successfully complete a background investigation in accordance with Homeland Security Presidential Directive-12 (HSPD-12) Office of Management and Budget (OMB) guidance M-05-24, M-11-11 “Continued Implementation of Homeland Security Presidential Directive (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors,” and as specified in agency-identified security directives and procedural guides.

The ordering agency will be responsible for the cost of any required background investigations.

C.1.8.8 National Policy Requirements

The concept of a national telecommunications infrastructure is recognized in national policy statements and directives issued under the authority of the Executive Office of the President, Congress, the Department of Homeland Security (including the Office of Emergency Communications), and other entities of the government. This telecommunications infrastructure is required to support the critical needs of the government under conditions of stress that range from crises and natural disasters (e.g., flood, earthquake) through declared conditions of National Security and Emergency Preparedness (NS/EP). Public safety and the economic well-being of the nation also depend upon the availability of reliable and responsive telecommunications services. EIS is a key component of the US national telecommunications infrastructure.

GSA expects to effectively provide assurance for government users that services and service elements (technical, management and operations-related) acquired through EIS will be in compliance with national policy throughout the life of the contracts. The contractor shall ensure that services delivered are in compliance with national policy directives that apply to the national telecommunications infrastructure.

Specific national policy requirements include, but are not limited to:

1. NS/EP requirements include a wide range of Executive Orders, Presidential Directives as promulgated by the Executive Office of the President, the Director of

Homeland Security, the Office of Emergency Communications and other government entities. NS/EP requirements are covered in Section G.11.

2. OMB Memorandum M-21-07 directs that agencies must transition from IPv4 agency infrastructures to IPv6 agency infrastructures (network backbones). For agencies with an IPv6 network (and those implementing IPv6 networks) the contractor solution must maintain functionality and shall comply with relevant policies and standards defined by OMB and NIST SP 500-267. All systems, software, and equipment supporting the agency network and its services shall handle IPv6 in an equivalent or more efficient method than IPv4 capabilities, performance, and security. No systems, software, or equipment shall be deployed on the network that does not meet this requirement. Additionally, all network management shall be enabled using IPv6.

3. OMB Memorandum M-19-26 rescinds previous memos for TIC Policy including M-08-05, M-08-16, M-08-27 and M-09-32 to reduce obstacles for “the adoption of cloud-based infrastructure.” M-19-26 further states: "…this memorandum provides an enhanced approach for implementing the TIC initiative that provides agencies with increased flexibility to use modern security capabilities. This memorandum also establishes a process for ensuring the TIC initiative is agile and responsive to advancements in technology and rapidly evolving threats.” OMB Memorandum M-15-01, “Fiscal year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices” requires Departments and Agencies (D/As) to enter into legally sufficient agreements with DHS relating to the deployment of EINSTEIN. DHS establishes these agreements with D/As authorizing in-line traffic inspection and modification, and such activities may include the interception, modification, use, and disclosure of D/A traffic. As such, specific EIS data service offerings: VPNS, Ethernet Transport, PLS, IPS, Cloud services, which includes IaaS Private Cloud, Paas, and SaaS, MNS Traffic Aggregation Service, MTIPS, and IPSS, and in future implementations could include other externally routed data services(e.g. OWS, SONETS), transporting Internet, Extranet, and Inter-Agency traffic shall identify and route said government traffic through a secure DHS EINSTEIN Enclave for processing by the latest generation of EINSTEIN capabilities. . The contractor shall design, implement, and operate its services to achieve the required routing of traffic through (including delivery to and receipt of traffic from) DHS EINSTEIN Enclaves. Transport SLA KPIs are measured as if through loopbacks in EINSTEIN Enclaves. EINSTEIN Enclaves are strictly intermediate hops and shall not be considered end points for SLA measurement. These contractor-performed actions related to EINSTEIN--whether performed for

DHS, GSA, or customer agencies--are intended to be assistance provided to the Secretary of DHS in accordance with 6 U.S.C. § 151.

4. In 2015, section 223 of the Federal Cybersecurity Enhancement Act of 2015 (the FCEA), Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242, Division N, Title II, Subtitle B (2015) (relevant portions codified at 6 U.S.C. §§ 151 and 151 note) created a statutory requirement for the Secretary of Homeland Security to "deploy, operate, and maintain" and "make available for use by any agency" capabilities to detect cybersecurity risks in agency network traffic and take actions to mitigate those risks. 6 U.S.C. § 151(b)(1). The FCEA also mandated that agencies deploy these capabilities fully on all perimeter network traffic. FCEA § 223(b) (6 U.S.C. § 151, note) ("[T]he head of each agency shall apply and continue to utilize the [above authorized intrusion detection and prevention] capabilities to all information traveling between an agency information system and any information system other than an agency information system."). To help enable these capabilities, the FCEA authorized DHS to "enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy, operate, and maintain technologies in accordance with [6 U.S.C. § 151(b)]"—the legal provision authorizing the capabilities. 6 U.S.C. § 151(c)(2). And, it provided that "[n]o cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to [6 U.S.C. § 151(c)(2].

5. In accordance with 6 USC 151(e)(1)(B), the contractor may not use any network traffic transiting or traveling to or from an agency information system to which the contractor gains access in accordance with 6 USC 151 for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to 6 U.S.C. § 151 (c)(2) or as part of another contract with DHS.
6. The contractor shall comply with DHS policies and procedures supplied by DHS, including those governing the operation of the intrusion detection and prevention capabilities provided pursuant to this contract, including DHS information handling guidelines regarding information obtained through operation of the intrusion detection and prevention capabilities provided pursuant 6 U.S.C. § 151.
7. The contractor shall verify in writing with DHS before providing EINSTEIN related capabilities, including as part of MTIPS, IPSS, MSS and Traffic Aggregation task orders to an Agency, that the Agency has signed the required Memorandum of Agreement (MOA) relating to deployment of EINSTEIN with DHS. This MOA is a legal requirement for DHS furnished capabilities which include EINSTEIN.

Telecommunications policy and the national telecommunications infrastructure are increasingly impacted by the convergence of telecommunications and information technology. Thus, policy directives in the areas of Electronic Government ("E-Gov"), Enterprise Architecture development, and Information Assurance, for example, may also have implications for telecommunications infrastructure. Additional policy requirements may be identified to the contractor. If contract modifications are required to meet new government-specific requirements, the contractor shall submit a technical approach and schedule for proposing these modifications to the CO per contract modification guidelines identified in Section J.4.

C.1.8.9 Technical Support

The contractor shall provide customer technical support as a component of each of its EIS services. For detailed requirements, please see Section G.6.2 Customer Service Office and Technical Support and Section G.6.4 Trouble Ticket Management.

C.2 Technical Requirements

C.2.1 Data Service

C.2.1.1 Virtual Private Network Service

C.2.1.1.1 Service Description

The contractor's Virtual Private Network Service (VPNS) shall provide secure, reliable transport of agency applications across the provider's high-speed unified multi-service IP-enabled backbone infrastructure.

C.2.1.1.1.1 Functional Definition

The main characteristic of VPNS is that all infrastructure and devices involved in implementing the VPN are owned by the contractor and located at the edge of the contractor's backbone. Tunnels terminate at the contractor's edge router.

The contractor shall use its backbone to establish three basic solutions for VPNS:

1. Intranet ─ provides secure tunnels between remote sites, using broadband or dedicated access.
2. Extranet ─ enables trusted business partners to gain access to corporate information via secure/encrypted tunnels, using broadband or dedicated access.
3. Remote Access ─ enables mobile/remote workers to gain access to secure corporate information via secure encrypted tunnels, such as IPsec and TLS.

The contractor shall accommodate and optimize an agency's applications to enable the network to accurately and consistently allow for traffic prioritization and cost efficiencies to support the following VPNS traffic types:

1. Time-critical traffic such as voice and video.
2. Business-critical traffic such as transactions.
3. Non-critical traffic such as email.

C.2.1.1.1.2 Standards

VPNS shall comply with the following standards.

1. OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors"
2. NIST Special Publication (SP) 800-46 Revision 1 "Guide to Enterprise Telework and Remote Access Security"
3. IETF RFCs:
    a) For secure VPNs:
        i. General IPSec
        ii. ESP and AH
        iii. Key exchange
        iv. Cryptographic algorithms to include but not limited to 3DES, RC4 and AES
        v. IPSec policy handling
        vi. IPSec MIBs
        vii. Remote access
        viii. Certification Authorities
    b) For trusted VPNs:
        i. General MPLS
4. IP Security Working Group – RFC 4303
5. IP Security Policy Working Group – RFC 3586
6. MPLS Working Group – RFC 3468
7. Layer 3 Virtual Private Network (L3VPN) Working Group – RFC 4176
8. Pseudo Wire Emulation Edge to Edge (pwe3) Working Group – RFC 3985
9. Use of PE-PE GRE or RFC4364 VPNs

10. IETF-TLS Working Group – RFC 5246 for TLS 1.2
11. TLS 1.2 Protocol Specification
12. IETF RFCs for IPv4 and IPv6
13. CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information Among National Security Systems
14. All new versions, amendments, and modifications to the above documents and standards

C.2.1.1.1.3 Connectivity

VPNS shall connect government locations and trusted business partners for site-to-site access or broadband for remote access to provide direct connectivity between all sites as a partially- or fully-meshed WAN.

C.2.1.1.1.4 Technical Capabilities

The following VPNS capabilities are mandatory unless marked optional.

1. The contractor shall meet applicable routing requirements in Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.
2. The contractor shall provide multiple tunneling standards, as required by an agency. Examples include L2TP, GRE, IP-in-IP, MPLS, IPSec, and TLS.
3. The contractor shall provide various encryption levels, as required by an agency. Examples include 3DES, RC4 and AES in accordance with the appropriate FIPS publications and modules.
4. The contractor shall provide authentication services as required by an agency. Examples include RADIUS, Internal LDAP, token integration, PKI, and X.509 certificates.
5. The contractor shall support IPv4 as both the encapsulating and encapsulated protocol.
6. The contractor shall support IPv6 as both the encapsulating and encapsulated protocol.
7. The contractor shall support QoS in the following standardized modes:
    a) Best effort
    b) Aggregate Customer Edge (CE) Interface level QoS (“hose” level)
    c) Site-to-site level QoS (“pipe” level)
    d) Intserv (RSVP) signaled

   e) Diffserv marked

8. The contractor shall support QoS across a subset of the access networks as listed below:

   a) 802.1p Prioritized Ethernet
   b) MPLS-based access
   c) Multilink Multiclass PPP
   d) QoS-enabled wireless:
      i. LTE, 5G and future evolutions
      ii. Wireless 802.11.x
      iii. Cable high-speed access (DOCSIS 1.1)
      iv. QoS-enabled Digital Subscriber Line (DSL)
      v. QoS-enabled Satellite Broadband Access

9. The contractor shall support one or more of the following application level QoS objectives:

   a) Intserv model for selected individual flows
   b) Diffserv model for aggregated flows

10. The contractor shall provide isolation of traffic and routing service that isolates the exchange of traffic and routing information to only those sites that are authenticated and authorized members of a VPN. The contractor shall provide layered security architecture to ensure that attackers will not find a single point of entry but will be faced with multiple layers of security.

11. The contractor shall support multiple VPNs by allowing both permanent and temporary access to one or more VPNs for authenticated users across a broad range of access technologies.

12. The contractor shall provide secure routing services to provide full routing capability on the VPN platform with a secure policy across the VPN.

13. The contractor shall support the inclusion of encryption, decryption, and key management profiles as part of the security management system.

14. The contractor shall support an agency in deploying its own internal security mechanisms in addition to those deployed by the contractor, in order to secure specific applications or traffic at a granularity finer than a site-to-site basis.

15. The contractor shall allow an agency to choose from alternatives for authentication of temporary access users. Authentication server choices include:

   a) Contractor-provided

b) Third party

c) Agency-provided

C.2.1.1.2 Features

The VPNS features are mandatory unless marked optional.

ID Number	Name of Feature	Description
1	High availability options	The contractor shall provide the following high availability options: 1. Load sharing 2. Fail-over protection 3. Diverse access points to service provider's POP(s).
2 (optional)	Interworking Services	The contractor shall provide interworking services for an agency's VPN to transparently access agency locations that use the contractor's Ethernet Transport Service.
3 (optional)	Cloud Service Provider Connection (CSPC)	The contractor shall provide encrypted (Std: FIPS Pubs: 140-2/3) cloud connection to agency specified public and/or private Cloud Service Provider(s) (CSPs), as follows: 1. Capacity and usage based connections: a) Fixed capacity and/or data usage based CSPC. b) Scalable bandwidths or bursting. Predefined committed bandwidth (CIR) with burstable bandwidths over the CIR (Overage) up to a maximum bandwidth, as specified in the task order and/or data consumption with a defined CIR 2. Connections to multiple CSPs. 3. Monitoring and management of CSPC (if available): This capability will allow customer to self-manage and monitor via web interface to: create/delete connections, change CIR and Overage amounts, open a trouble ticket, access utilization reports, view order history, and view unbilled usage and usage reports. 4. Security. If additional security is required by an agency task order, solutions may utilize EIS Managed Security Service (MSS) through "service chaining," for example, firewall, intrusion detection, and intrusion prevention services.

C.2.1.1.3 Interfaces

These UNIs at the SDP for VPNS are mandatory unless marked optional.

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type (See Note 1)
1	Ethernet Interface	1 Mbps up to 10/40/100 Gbps or higher (Std IEEE802.3ae and 802.3ab)	IPv4/v6 over Ethernet
2	Private Line Service	1. DS0 2. T1 3. T3 4. OC-3c 5. OC-12c 6. OC-48c 7. OC-192c 8. OC-768c (optional)	IPv4/v6 over PLS
3	IP over SONET Service	1. OC-3c 2. OC-12c 3. OC-48c 4. OC-192c 5. OC-768c (optional)	IP/PPP over SONET
4	DSL Service	xDSL access at 1.5 Mbps download and above, and 384 Kbps and above upload	Point-to-Point Protocol, IPv4/v6
5 (optional)	Cable high speed access	25 Mbps download, 5 Mbps upload and above (DOCSIS 3.x or latest standard)	Point-to-Point Protocol, IPv4/v6
6	Wireless Access	1. Wi-Fi 2. LTE, 5G and future evolutions 3. Satellite	Point-to-Point Protocol, IPv4/v6

Notes:

1. IPv6 shall be supported by the contractor.
2. Where E-1/E-3 carrier service is provided, appropriate corresponding payload data rates apply.

C.2.1.1.4 Performance Metrics

The performance levels and acceptable quality level (AQL) of KPIs for VPNS are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Latency (CONUS)	Routine	70 ms	≤ 70 ms	See Note 1
Latency (OCONUS)	Routine	150 ms	≤ 150 ms	See Note 2

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Av(VPN)	Routine	99.9%	≥ 99.9%	See Note 3
	Critical	99.99%	≥ 99.99%	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 4
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Latency value is the average round trip transmission between agency premises routers for an VPN with all of its CONUS sites. The latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods. Relevant standards are RFC 1242 and RFC 2285. The contractor may propose to the government more cost-effective test and measurement technique alternatives that meet or exceed the requirements in RFC 1242 and RFC 2285.
2. Latency value is the average round trip transmission between agency premises routers for an IP VPN with its CONUS and OCONUS sites. The latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods. Relevant standards are RFC 1242 and RFC 2285. The contractor may propose to the government more cost-effective test and measurement technique alternatives that meet or exceed the requirements in RFC 1242 and RFC 2285.
3. VPN availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the VPN is operationally available to the agency. Availability is computed by the standard formula:

$$Av(VPN) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

4. See Section G.8.2 for the definitions and measurement guidelines.

C.2.1.2 Ethernet Transport Service

C.2.1.2.1 Service Description

Carrier Grade Ethernet transport service shall be implemented over an MPLS backbone, where Ethernet links are transported using MPLS label switched paths (LSPs) inside an outer MPLS “tunnel.” Point-to-point connections can also be provided by Ethernet over SONET solutions.

Ethernet Transport Service (ETS) allows agencies to interconnect their LANs (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 or higher Gbps) transparently over the Metro Area Networks (MAN) and the Wide Area Networks (WAN) regardless of the geographical location of their sites. Ethernet Transport Service enables Intranet and Extranet services, as well as intra- and inter-agency communications.

Ethernet shall be provided as a dedicated service or a shared service. Dedicated Ethernet is defined as private services that are carried over dedicated facilities at fixed and predetermined speeds. Shared Ethernet is defined as statistically multiplexed Ethernet connections.

C.2.1.2.1.1 Functional Definition

ETS provides point-to-point, point-to-multipoint and multipoint-to-multipoint connections. ETS exploits Ethernet's flexibility, cost effectiveness, and differentiation of service (e.g., traffic priority) capabilities while providing end-to-end transport of data traffic with minimal protocol conversion. The following ETS shall be supported:

1. **Ethernet Private Line (E-LINE)**. E-Line is a point-to-point service in which bandwidth is reserved. E-Line supports full port speeds (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 or higher Gbps) and can support different quality of service (QoS) priorities for customer traffic. E-Line is a point-to-point configuration as a Layer 2 tunnel providing a transparent dedicated connection between two sites. This service resembles/replaces traditional Time Division Multiplexing (TDM) private line service. Some applications include router interconnect, business continuity, and disaster recovery. E-LINE service can be offered over the MAN and/or WAN.
2. **Ethernet Private LAN (E-LAN**). E-LAN supports both point-to-multipoint and multipoint-to-multipoint configurations. For point-to-multipoint configurations, ETS connects three or more sites over Layer 2 tunnels. It supports full port speeds (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 or higher Gbps) and can support different QoS priorities for customer traffic. For multipoint-to-multipoint configuration, also called E-Tree service, ETS connects several sites, similar to point-to-multipoint configuration, by connecting one or more roots and a set of leaves, but preventing inter-leaf communication. More than one site can be configured as the root site and other sites can communicate with each other through multiple root sites; for example, connecting disparate LAN segments into a single agency-wide virtual LAN. E-LAN can be offered over the MAN and/or WAN.

C.2.1.2.1.2 Standards

ETS shall comply with the following standards:

1. Metro Ethernet Forum (MEF CE 3.0):
    a) (Optional) Support Jumbo Ethernet frames
    b) CE 3.0 is set of MEF CE 3.0 Certified network elements that connect to transport Carrier Ethernet services for all users, locally and worldwide. Ethernet transport services are carried over physical Ethernet networks and other legacy transport technologies.
    c) Key Specifications:
        - MEF 6.3 - Subscriber Ethernet Service Definitions
        - MEF 10.4 - Subscriber Ethernet Service Attributes
        - MEF 33 - Ethernet Access Services
        - MEF 23.2 – Carrier Ethernet Class of Service – Phase 3
        - MEF 26.2 - ENNI and Operator Service Attributes
    d) CE 3.0 expands CE 1.0 to:
        - 8 services, 2 of each respectively in E-Line, E-LAN, E-Tree, and E-Access (defined in MEF Standards MEF 6.1, 22.1, 33)
        - Standardized Multi-CoS with application-oriented CoS Performance Objectives, new metrics (MEF 6.3, 10.4, 20, 23.2)
        - Interconnect through the integrated delivery of MEF Service Attributes (MEF 10.4, 26.2, 33) allows ubiquitous deployment spanning multiple providers
        - Manageability, (MEF 7.3, 16, 17, 30.1, 31) plus additional specifications
2. International Telecommunications Union (ITU):
    a) *Network architecture*:
        - G.8010/Y.1306 Architecture of Ethernet layer networks
    b) *Services:*
        - G.8011/Y.1307 Ethernet over Transport – Ethernet services framework
        - G.8011.1/Y.1307.1 Ethernet private line service
        - G.8011.2/Y.1307.2 Ethernet virtual private line service
        - G.8011.3/Y.1307.3 Ethernet virtual private LAN service (draft)
        - G.8011.4/Y.1307.4 Ethernet virtual private rooted multipoint service (draft)
        - G.8012/Y.1308 Ethernet UNI and Ethernet NNI
    c) *OAM*:

- Y.1730 Requirements for OAM functions in Ethernet-based networks and Ethernet services
- Y.1731 OAM functions and mechanisms for Ethernet-based networks

d) *Protection:*

- G.8031/Y.1342 Ethernet linear protection switching
- G.8032/Y.1344 Ethernet ring protection switching

e) *Equipment:*

- G.8021/Y.1341 Characteristics of Ethernet transport network equipment functional blocks

f) *Equipment management:*

- G.8051/Y.1345 Management aspects of the Ethernet-over-Transport (EoT) capable network element

g) *Terminology:*

- G.8001/Y.1354 Terms and definitions for Ethernet frames over Transport (EoT)

3. Institute of Electrical and Electronics Engineers, Inc. (IEEE):

a) IEEE 802.3 (as updated from time to time by IEEE), 1Gbps LAN PHY, 10Gbps LAN PHY, 10Gbps WAN PHY
b) IEEE 802.3ae (as updated from time to time by IEEE), 10Gbit Ethernet 802.17, Resilient Packet Rings (RPR) – in progress
c) IEEE 802.1ah (as updated from time to time by IEEE), Ethernet First Mile
d) IEEE 802.1p (as updated from time to time by IEEE)
e) IEEE 802.1q (as updated from time to time by IEEE)

4. Acceptance Testing of ETS:

a) RFC 2544
b) RFC 6815

5. All new versions, amendments, and modifications to the above documents and standards

C.2.1.2.1.3 Connectivity

ETS shall connect to and interoperate with:

1. **Intra-agency LAN-LAN Connectivity.** ETS provides connectivity for an agency's LANs located in the same city or different cities, thereby extending the LAN to the MAN and WAN. This is achieved by connecting the agency's SDP(s) in one

location to another SDP(s) in one or more locations. Interconnection shall be possible over transoceanic links, if required.

2. **Inter-agency LAN-LAN Connectivity**. Different agencies may share resources to connect to the contractor's metro or long haul network. This is achieved by connecting from one agency's SDP(s) to other agencies' SDP(s).

C.2.1.2.1.4 Technical Capabilities

The following ETS capabilities are mandatory unless marked optional:

1. The contractor shall meet applicable routing requirements in Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.
2. Geographical Coverage. A seamless end-to-end service shall be provided from the SDP Customer Premise Equipment (CPE) traversing the contractor's network (Metro Access/Core and Long Haul) in order to minimize conversion of protocols. The contractor shall indicate if protocol conversions are required and how they impact the delay when delivering services end-to-end. The following geographical coverage shall be provided:
   a) Intra-City ETS – the contractor shall provide Ethernet connections to agency sites located in the same city inside the US (CONUS and Metro) and outside the US (OCONUS and Non-Domestic).
   b) Inter-City ETS – Ethernet connections shall be delivered at domestic and non-domestic locations (CONUS/Metro, OCONUS/Non-Domestic).
3. The contractor shall support Ethernet UNI (User-to-Network-Interface) to support Layer 2 and Layer 3 clients. Layer 3 clients are agency devices that support Layer 3 protocol packets such as IPv4, IPv6.
4. The contractor shall support Ethernet Virtual Connections (EVCs).
5. The contractor shall support delivery of the ETS at the agency's Service Delivery Point (SDP) via a UNI.
6. If required, the contractor shall support circuit emulation services for TDM services.
7. The contractor shall support point-to-point, multipoint-to-multipoint, and Rooted multipoint EVCs.
8. EVC multiplexing shall be supported.
9. The contractor shall support rate-limited throughput access links, i.e., 1 Gbps port rate limited in 100 Mbps increments.
10. The contractor shall support rate-limiting at the agency's SDP and at the individual VLAN ingress and egress.

11. Privacy and security shall be supported per IEEE 802.3 (as updated from time to time by IEEE) and as defined in the TO.
12. The contractor shall support the following service attributes:
    a) Physical interfaces shall be supported as listed in Section C.2.1.2.3
13. The following traffic profiles shall be supported:
    a) Committed Information Rate (CIR) – minimum amount of bandwidth guaranteed for an ETS
    b) Committed Burst Size (CBS) – the size up to which subscriber traffic is allowed to burst and still be in-profile and not discarded or shaped
    c) Peak Information Rate (PIR) – specifies the rate above the CIR that traffic is allowed into the network for a given burst interval defined by the MBS
    d) Maximum Burst Size (MBS)
14. Performance parameters shall be supported as listed in Section C.2.1.2.4.
15. Service Frame Delivery options supported shall include:
    a) Unicast Frame Delivery
    b) Multicast Frame Delivery, as per RFC 4604
    c) Broadcast Frame Delivery as per IEEE 802.3 (as updated from time to time by IEEE)
16. VLAN tag supported shall include:
    a) VLAN tag preservation
    b) VLAN tag translation
    c) VLAN tag stacking
    d) VLAN aggregation across a common physical connection (optional)
17. Service multiplexing shall be supported to include multiple EVCs connected via a single UNI.
18. Bundling shall be supported to enable two or more VLAN IDs to be mapped into a single EVC at a UNI.
19. Security Filters shall be supported as specified in the TO.
20. (Optional) The contractor shall provide proactive Performance Monitoring (PM). It is desirable that all items in the following list be supported:
    a) Signal failure
    b) Signal degradation
    c) Connectivity or Loss of connectivity

   d) Frame loss
   e) Errored frames
   f) Looping
   g) Denial of service (DoS)
   h) Misinserted frames
   i) Maintenance parameters

21. The contractor shall support the following maintenance functions:
    a) Alarm suppression
    b) Loopbacks (intrusive and non-intrusive (transparent to on-going connections))
    c) Protection switching, restoration, etc.
22. The contractor shall support the following network topologies:
    a) Point-to-point
    b) Rooted Multipoint
    c) Multipoint-to-Multipoint (i.e., mesh)
23. The contractor shall support geographical diversity to provide added reliability. An agency may buy a geographical diverse route from the same or a different contractor to serve as a protection path.
24. The contractor shall support bridging in compliance with IEEE 802.1Q (2014).
25. The contractor shall support the following Virtual Connection sizes:
    a) For point-to-point Ethernet connections
    b) For multi-point-to-multi-point connections
26. Quality of Service (QoS) – The contractor shall support traffic prioritization that enables higher priority traffic to be transmitted first.
27. The contractor shall support traffic reconfiguration that supports the ability of the agency to modify a specific service connection subsequent to the establishment of the connection. Changes to an established connection may include upgrade/downgrade of speeds that do not result in physical equipment changes.

C.2.1.2.2 Reserved

C.2.1.2.3 Interfaces

The UNIs at the SDP are mandatory unless marked optional:

UNI Type	Interface Type	Standard (as updated from time to time by IEEE)	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling Protocol Type/Granularity
1	Optical	IEEE 802.3z	1310 nm	1 Gbps	Gigabit Ethernet
2	Optical	IEEE 802.3z	850 nm	1 Gbps	Gigabit Ethernet
3 (optional)	Optical	IEEE 802.3	1310 nm	100 Mbps	Fast Ethernet
4 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm	10/40/100 Gbps	10/40/100GBASE-SR (65 meters)
5 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	850nm	10/40/100 Gbps	10/40/100GBASE-SW
6 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1550 nm	10/40/100 Gbps	10/40/100GBASE-ER
7 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm	10/40/100 Gbps	10/40/100GBASE-LR
8 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1550 nm	10/40/100 Gbps	10/40/100GBASE-LW
9 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1300 nm Multimode	10/40/100 Gbps	CWDM 10/40/100GBASE-LX4 (300 meters)
10 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm Single Mode	10/40/100 Gbps	CWDM 10/40/100GBASE-LX4 (10,000 meters)
11 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm Single Mode	10/40/100 Gbps	10/40/100GBASE-LW (10,000 meters)

UNI Type	Interface Type	Standard (as updated from time to time by IEEE)	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling Protocol Type/Granularity
12 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1550 nm Single Mode	10/40/100 Gbps	10/40/100GBASE-EW (40,000 meters)
13 (optional)	Electrical	IEEE 802.3	N/A	10 Mbps	10Base
14	Electrical	IEEE 802.3	N/A	100 Mbps	100 Base
15	Optical	IEEE 802.3		1 Gbps	1000Base
16 (optional)	Optical	ITU-T G.707	1300 nm	STM-4	SDH STM-1, VC-11 (DS1), VC-12 (E1), VC-3 (DS3, E3, other), VC-4
17 (optional)	Optical	ITU- G.707	1300 nm	STM-4c	VC-4-4c
18 (optional)	Optical	IEEE 802.3z IEEE 802.3ab	Multimode	1 Gbps	1000BASE-LX
19 (optional)	Optical	IEEE 802.3z IEEE 802.3ab	Multimode	1 Gbps	1000BASE-SX
20 (optional)	Electrical (Copper)	IEEE 802.3z	N/A	1 Gbps	1000BASE-CX
21 (optional)	Electrical (Twisted pair)	IEEE 802.3z	N/A	1 Gbps	1000BASE-T
22 (optional)	Optical	GR-253, ITU-T G.707	1310 nm	10/40 Gbps	SONET or SDH

C.2.1.2.4 Performance Metrics

The performance levels and AQL of KPIs for ETS are mandatory unless marked optional:

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Av (ETS)	Routine (Single Connection)	99.9%	≥ 99.9%	See Note 1
	Critical (Double Connection)	99.99%	≥ 99.99%	
Latency (ETS)	CONUS	100 ms	≤ 100 ms	See Note 2
	OCONUS	200 ms	≤ 200 ms	
Jitter (Packet)	Routine	10 ms	≤ 10 ms	See Note 3
Grade of Service (Packet Delivery)	Routine	99.95%	≥ 99.95% at all times	See Note 4
	Critical	99.99%	≥ 99.99% at all times	
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 5
	With Dispatch	8 hours	≤ 8 hours	
Grade of Service (Fail Over Time)	Routine	1 minute	1 minute	See Note 6
	Critical	100 ms	≤ 100 ms	See Note 6

Notes:

1. ETS availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the ETS is operationally available to the agency. Availability is computed by the standard formula:

$$Av(EthS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Latency is the round trip delay experienced by an end user across the contractor's network to other agencies' sites. It is the average time for packets to travel over the core network. The Internet Control Message Protocol (ICMP) test can be used to calculate packet delivery and latency. The ICMP test consists of sending, every five minutes, a series of five test packets between originating agency's SDPs and the delivery SDPs. The test results are analyzed to determine packet loss vs. successful delivery and speed of delivery. Contractor shall meet or exceed standards set by RFC 1242 and RFC 2285. It can be determined by the following formula: (Distance/(0.6*c)+hops*delay), where c is the velocity of light and 0.6 is the multiplier recommended by the ITU (G.144) in ms/km plus the delay in each hop caused by the routers times the number of hops.
3. Measurements of packet jitter are performed by injecting packets at regular intervals into the network and measuring the variability in the arrival time. Relevant standard is RFC 2679.
4. Network devices, such as switches and routers, sometimes have to hold data packets in buffered queues when a link gets congested. If the link remains congested for too long, the buffered queues will overflow and data will be lost. The loss can be measured with the ICMP test. The contractor is expected to meet or exceed relevant standards such as RFC 1242 and RFC 2285.
5. As per GR-418. Refer to Section G.8.2 for definitions and how to measure.
6. Restoration for links transported over the Ethernet infrastructure (i.e., Ethernet switches) is achieved by the use of protocols such as Spanning Tree (IEEE 802.1d), which converge more slowly than SONET. Therefore, ETS for critical users shall be delivered over a carrier class infrastructure.

C.2.1.3 Optical Wavelength Service

Government agencies require dedicated broadband, framing-independent transport networks to interconnect their offices in different regions of the United States and internationally. In offering Optical Wavelength Service (OWS), the contractor always provides the optical electronics (optronics) equipment and fiber connectivity that comprise the transport network. Management of the network, however, may be performed by either the contractor or the agency. In the latter case, agencies will manage their dedicated networks via a Web portal or a remote user interface.

C.2.1.3.1 Service Description

The method of providing OWS is Wavelength Division Multiplexing (WDM).

OWS delivered over WDM provides a high-bandwidth solution without the cost of owning and operating network infrastructure.

OWS is provided over WDM equipment where several wavelengths, or lambdas, are multiplexed into a composite signal that is transported over a single fiber. The composite signal is then de-multiplexed at the receiver end and each wavelength is recovered.

C.2.1.3.1.1 Functional Definition

Basic OWS is a point-to-point, bi-directional, single link service delivered over WDM.

C.2.1.3.1.2 Standards

OWS over WDM shall comply with the following standards, as applicable:

1. ITU Standards defining frequencies grid and physical layer parameters for WDM are G.692 and G.694.
2. ITU Standards defining frequencies grid for CWDM are G.694.2.
3. (Optional) ITU Standards defining OTN architecture, interface formats, and physical layer interfaces are G.872, G.709, and G.959.1 respectively.
4. Applicable ITU Standards defining submarine transmission functional requirements are G.971, G.972, G.973, G.974, G.975, G.976 and G.977.
5. Telcordia standards for metro and long haul protection are GR-253, GR-1400, and GR-1230.
6. Telcordia standard for reliability assurance is GR-418.
7. Applicable Telcordia for WDM systems are GR-1073, GR-1312, GR-2918, GR-2979 and GR-3009.
8. VSR4-01 (OC-192 Very Short Reach Interface, 12 fibers 850nm)
   OIF-VSR4-01.0 - Very Short Reach (VSR) OC-192 Interface for Parallel Optics (optional).
9. VSR4-02 (OC-192 Very Short Reach Interface, 1 fiber 1310nm)
   Note: VSR4-02 has been included as the 4dB link option in VSR4-05 below (optional).

10. VSR4-03.1 (OC-192 Very Short Reach Interface, 4 fibers 850nm) OIF-VSR4-03.0 - Very Short Reach (VSR) OC-192 Four Fiber Interface Based on Parallel Optics (optional).
11. VSR4-04 (OC-192 Very Short Reach Interface, 1 fiber 850nm) OIF-VSR4-04.0 - Serial Shortwave Very Short Reach (VSR) OC-192 Interface for Multi-mode Fiber (optional).
12. VSR4-05 (OC-192 Very Short Reach Interface, OXC 1310nm) OIF-VSR4-05.0 - Very Short Reach (VSR) OC-192 Interface Using 1310 Wavelength and 4 and 11 dB Link Budgets (optional).
13. VSR5-01 (OC-768 Very Short Reach Interface) OIF-VSR5-01.0 - Very Short Reach Interface Level 5 (VSR-5): OWS OC-768 Interface for Very Short Reach (VSR) Applications (optional).
14. All new versions, amendments, and modifications to the above documents and standards.

C.2.1.3.1.3 Connectivity

OWS shall be delivered at the Service Delivery Point (SDP) via UNIs as specified in Section C.2.1.3.3.

Point-to-point, bi-directional, duplex services shall be connected from the SDP to the Optical Transport Network via a fiber pair.

The wavelengths ordered by the agencies shall connect to and interoperate with:

1. Contractor's metro and long haul networks
2. Agency's Intranet
3. Other agency networks

C.2.1.3.1.4 Technical Capabilities

The following OWS capabilities are mandatory unless marked optional:

The contractor shall support the following three types of connections:

1. **Non-domestic Wavelengths (optional)**. The contractor shall support international wavelengths that may be part of an end-to-end service or a stand-alone connection. An end-to-end wavelength service shall drop and pick up traffic from and to locations, as required by an agency:
   a) Backhaul services shall be available where necessary.

b) The basic service shall be a single point-to-point; bi-directional wavelength connecting two sites.

2. **Domestic Wavelengths**. The contractor shall support wavelengths over the long-haul network. This is applicable for inter-city connectivity within the United States and territories not in the continental US.

   The basic service shall be a single point-to-point, bi-directional wavelength connecting two agency sites located in different states.

3. **Metro Wavelength Services**. The contractor shall support the provisioning of wavelengths over its metro networks.

   Single point-to-point, bi-directional wavelengths connecting two agency sites in the same city shall be supported.

The contractor shall provide the following capabilities:

1. **Transmission Rates**. Wavelengths shall be supported at 1 Gbps, 2.5 Gbps, and 10 Gbps. The contractor has the option to also support wavelengths at 40 Gbps and 100 Gbps. Following the implementation of EIS, the contractor may support additional optional rates beyond 100 Gbps if and when such transmission rates become available.
2. **Clock Transparency**. The contractor's networks shall support the following levels of clock transparency:
   a) Asynchronous transport, where the contractor's network shall not apply clocking to the agency's traffic
   b) The contractor's network shall provide Synchronous Status Messaging (SSM) byte transparency
3. **Protocol Transparency - Metro**. The contractor shall support Metro wavelengths that are rate and protocol independent.
4. **Protocol Transparency – Domestic and Non-Domestic**. The contractor shall support Domestic and Non-Domestic Wavelengths that are rate and protocol independent. (optional)
5. **Byte Transparency**. The support to framed wavelengths shall include byte transparency where the overhead bytes are passed through without being overwritten (i.e. non-intrusive Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) processing of the signals).
   a) Transparency of Transport Overhead (TOH) bytes shall be provided, with the exception of A1 and A2 bytes, B0 and J1. A1 and A2 are framing bytes which monitor the framing integrity of the incoming Synchronous Transport Signal

Level-N (STS-N, where N=1, 3, 12, 48, 192, 768) and Optical Carrier Level-N (OC-N, where N=1, 3, 12, 48, 192, 768) signals. The framing bytes can be terminated.

b) If the framed wavelengths supported are not fully transparent, the contractor shall indicate the level of transparency offered for wavelengths at 2.5 Gbps, 10 Gbps and 40 Gbps.

c) Fully transparent wavelengths shall be supported at 40 Gbps. This applies to Non-domestic, domestic, and metro wavelengths.

6. **Concatenation**. For framed wavelengths, the contractor shall support standard and virtual concatenation.

7. **(Optional) Channelization.** For framed wavelengths, the contractor shall support channelized UNIs.

8. **Wavelength Delivery.** Hand-off at the SDP shall be accomplished using two fibers over two ports when delivering bidirectional wavelength services, with one fiber for each direction. Patch panel and fiber terminations will be based on agency needs.

9. **Access Methods**. The contractor shall provide access methods to the ordered wavelength service for an end-to-end offering.

   a) If the contractor is not able to provide access on its network, it shall indicate what alternatives exist to enable the service end-to-end.

   b) Each end of the wavelength shall be delivered using access methods as required by the agency.

   c) When agency access is provided via the backbone of the Long Haul (LH) DWDM systems and is not collocated, the contractor shall specify the appropriate reach of the optical interface to be used. If the distance is too long for interfaces such as FICON, Fibre Channel, etc., the mediation devices or gateways needed shall be specified in order to compensate for distance limitations.

10. **Government Furnished Property (GFP) / SRE**. The contractor shall provide multi-vendor interoperability support to the GFP/SRE by completing connectivity using the appropriate UNIs in the following cases:

   a) Should the GFP/SRE and the metro WDM system be collocated at the agency's office, connectivity between them shall be established using Short Reach (SR) interfaces (1310 nm) or Very Short Reach (VSR).

   b) Should the GFP/SRE and the metro WDM systems be not collocated; the metro WDM shall be located in a telehouse or collocation hotel. In this case, the contractor shall interface with the GFP/SRE using the appropriate optical interface that shall reach the distance between the agency's office and the collocation site.

c) The wavelength service shall be able to support different kinds of traffic depending on the type of GFP/SRE (i.e., Fiber Connectivity (FICON), Enterprise System Connection (ESCON), and Fibre Channel for a Storage Area Network (SAN)).

11. **Efficient Transport**. The contractor shall ensure that a single wavelength is capable of transporting different types of traffic without the need to use a separate physical wavelength to run IP, Ethernet, etc.

C.2.1.3.2 Features

The following Optical Wavelength Service (OWS) over WDM features are mandatory, unless marked optional:

ID Number	Name of Feature	Description
1 (Optional)	Customer Network Management (CNM) – Level 1	The contractor shall provide monitoring capabilities only via this feature. Agency personnel shall be able to monitor wavelength(s) via alarm messages from the Optical Transport Network into a software user interface via a dashboard or an API from the agency network management system.
2 (Optional)	Customer Network Management (CNM) – Level 2	The contractor shall provide management and monitoring capabilities. These shall be included to support an alarm messages visibility and execution of control commands that shall be sent into the wavelength(s). Operations available shall include set up, modification and tearing-down connections.
3	Equipment Protection 1:1 – GFP/SRE	The contractor shall provide protection to the client interfaces at the SDP, where the protection channel is bridged to the failed working channel.
4	Equipment Protection 1+1 – GFP/SRE	The contractor shall provide protection to the User to Network Interfaces at the SDP, where the protection channel is permanently bridged to the working channel. Protection switching is faster than 1:1.
5	Equipment protection – Network Side	The contractor shall support two channels facing the network for full redundancy and equipment protection at the SDPs.

ID Number	Name of Feature	Description
6	Geographical Diversity Wavelengths	The contractor shall support geographically diverse wavelengths to be used by the agency as a hard protection against fiber failures. The configuration and exact diversity requirements, such as single/dual site delivery, single or dual metro hub, will be specified in the TO.
7 (Optional)	Protected Non-Domestic and OCONUS Wavelength	The contractor shall support protected Non-Domestic and OCONUS Wavelengths. These shall be architected using submarine transmission protocols such as Bidirectional Path Switched Ring (BPSR) or equivalent. The contractor shall ensure protection switching in the submarine transmission networks to be less than 4 seconds for a single failure.
8 (Optional)	Protected CONUS Wavelength	The contractor shall support protected CONUS Wavelengths using transmission protocols to provide resiliency. Protection switching in the nationwide transmission networks shall be less than 300 ms for a single failure. This feature is limited to 2,500 kilometers.
9	Protected Metro Wavelength	The contractor shall provide protection on a per-wavelength basis when delivering services in the metro areas, such as Unidirectional Path Switched Ring (UPSR). Restoration times for protected wavelengths in the metro area shall be below 60 ms for a single failure. When delivering protected wavelengths in the metro area, the agency and the contractor shall agree on whether equipment protection is required facing the GFP/SRE. If so, the contractor shall provide protection at the SDP and multiple UNIs shall be ordered, the number of which shall depend on the protection method selected by the agency. The contractor shall supply its own physical UNIs.

C.2.1.3.3 Interfaces

The existing UNIs at the SDP are mandatory unless marked optional:

UNI Type	Interface Type	Standard	Frequency of Operation	Payload Data Rate or Bandwidth	Signaling or Protocol Type
1	Optical	GR-253, ITU-T G.707	1310 nm	2.5Gpbs	SONET or SDH
2	Optical	GR-253, ITU-T G.707	1310 nm	2.5Gbps	SONET or SDH Concatenated
3	Optical	GR-253, ITU-T G.707	1310 nm	10Gbps	SONET or SDH
4 (optional)	Optical (over 12 fibers)	OIF-VSR4-01.0	850 nm	10 Gbps (12 fibers)	SONET or SDH
5 (optional)	Optical (over 1 fiber)	OIF VSR4-02	1310nm	10 Gbps (1 fiber)	SONET or SDH
6 (optional)	Optical (over 4 fibers)	OIF-VSR4-03.0	850nm	10 Gbps (4 fibers)	SONET or SDH
7 (optional)	Optical (over 1 fiber)	OIF-VSR4-04.0	850 nm	10 Gbps (1 fiber)	SONET or SDH
8 (optional)	Optical	OIF-VSR5-01.0	850 nm	40 Gbps	SONET or SDH

C.2.1.3.4 Performance Metrics

1. Framed Wavelength Performance – Wavelengths based on SONET framing shall comply with performance requirements as stated in Section C.2.1.5.1.4 (7) through (8).
2. Transparent Wavelength Performance – If applicable, the contractor shall describe the methods by which fully transparent wavelengths (i.e. based on all optical gear, G.709 based) will be monitored and how AQLs will be met.
3. The contractor shall support In-Service Monitoring (ISM) and shall not rely on performance observed and measured at higher layers of the network.

The Performance Levels and AQL of KPIs for OWS over WDM are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Av(OWS over WDM)	Routine	99.9%	≥ 99.9%	In-Service Monitoring See Note 1
	Critical	99.99%	≥ 99.99%	
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	
Grade of Service (Restoration Time)	Routine	100 ms	≤ 100 ms	In-Service Monitoring See Note 3
	Critical	60 ms	≤ 60 ms	

Notes:

1. OWS availability shall be measured in service on an end-to-end basis. COT(HR) shall be calculated based on errored seconds and/or severely errored seconds (SES) as defined by GR-253, G.826 through G.829 and shall be expressed in Hours. Availability is computed by the standard formula:

$$Av(OWS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section G.8.2 for definition and how to measure.
3. Restoration time is the time taken to reroute the traffic over a redundant path before the failure is repaired. For critical user traffic, the redundant path should be a geographically diverse wavelength in a 1+1 configuration where the time accounted for includes the switching time and the propagation time in the fiber.

Proactive monitoring using element management systems should be used to measure restoration time in real time. Simulation tools are also available and used by contractors. Calculated based on an 8000 km ring using the following formula: T= Detect time + Time in fiber + Time in Nodes + Time to bridge and switch + Traffic delay time. Domestic networks are usually ring based on the backbone. For 1+1 protection based on APS, GR-253 compliance includes 10 ms for detection and 50 ms for the actual switching.

C.2.1.4 Private Line Service

C.2.1.4.1 Service Description

Private Line Service (PLS) provides dedicated, reliable full-duplex bandwidth for agency-specific data networks and mission critical applications. The ranges of line speeds and reliability options provided by this service allow government users to satisfy an array of diverse requirements. This service can be used for various applications such as voice, data, video, multimedia, and encrypted communications.

C.2.1.4.1.1 Functional Definition

PLS provides dedicated duplex transmission connectivity between two or more designated end points over which agency service applications traverse at agency-specified bandwidths. The connectivity between the end points is permanently established unless a service request is received for a modification, move, or disconnect.

C.2.1.4.1.2 Standards

PLS shall comply with the following standards:

1. ANSI T1.102/107/401/403/503/510 for T1
2. Telcordia PUB GR-499-CORE for T3
3. ANSI T1.105 and 106 for SONET
4. Telcordia PUB GR-253-CORE for SONET
5. ITU-TSS G.702 and related Recommendations for E1 and E3
6. Telcordia PUB SR-TSV-002275, TR-NWT-000965, and TR-NWT-000335 for analog
7. Telcordia PUB GR-418-CORE for reliability/performance

C.2.1.4.1.3 Connectivity

PLS shall connect to and interoperate with:

1. Government-specified terminations (e.g., SDPs such as PBXs, Multiplexers, Routers, Video CODECs, and Group 4 FAXs)
2. All other networks including other EIS contractors' networks, where additional coordination between networks will be required for interoperability

C.2.1.4.1.4 Technical Capabilities

The following PLS capabilities are mandatory unless marked optional:

1. The contractor shall meet applicable routing requirements in Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.
2. Transparency to any protocol used by GFP.
3. Data transparency treatment of all bit sequences transmitted by GFP through the SDP.

The contractor shall support the following categories (i.e., data rates) of PLS service:

1. **DS0**. Information payload data rates of 56 Kbps and 64 Kbps.
2. **T1**. Line rate of 1.544 Mbps, which may be used to provide channelized or un-channelized T1 service as follows:
    a) Channelized T1. In this mode, 24 separate DS0s clear channels of either 56 Kbps or 64 Kbps shall be supported.
    b) Un-channelized T1. In this mode, a single 1.536 Mbps information payload shall be supported.
3. **T3**. Line rate of 44.736 Mbps, which may be used to provide channelized or un-channelized T3 service as follows:
    a) *Channelized T3*. In this mode, 28 separate DS1 channels of 1.536 Mbps information payload rate shall be supported.
    b) *Un-channelized T3*. In this mode, a single 43.008 Mbps payload shall be supported.
4. **E1**.. Line rate of 2.048 Mbps, which may be used to provide channelized or un-channelized E1 service as follows:
    a) *Channelized E1*. In this mode, 30 separate DS0 clear channels shall be supported.
    b) *Un-channelized E1*. In this mode, a single 1.92 Mbps information payload shall be supported.
5. **E3**. Line rate of 34.368 Mbps, which may be used to provide channelized or unchannelized E3 service as follows:

  a) *Channelized E3.* In this mode, 16 separate E1 channels shall be supported.
  b) *Un-channelized E3* In this mode, a single 30.72 Mbps information payload shall be supported.

6. **(Optional) SONET OC-1**. Single SONET OC-1 channel with the information payload data rate of 49.536 Mbps over an interface with a line rate of 51.840 Mbps.
7. **(Optional) SONET OC-1**. Virtual Tributary. Seven Virtual Tributary (VT) groups over a single SONET OC-1 interface with a line rate of 51.840 Mbps. Each VT group shall be able to independently carry four T1 or two DS1C or one DS2 channel(s); where each T1 has a line rate of 1.544 Mbps and payload data rate of 1.536 Mbps, and each DS1C has a line rate of 3.152 Mbps and information payload data rate of 3.072 Mbps, and each DS2 has a line rate of 6.312 Mbps and information payload data rate of 6.144 Mbps.
8. **SONET OC-3**. Line rate of 155.520 Mbps, which may be used to provide channelized OC-3 or concatenated OC-3c service as follows:
   a) *Channelized OC-3*. In this mode, three separate OC-1 channels, each with an information payload data rate of 49.536 Mbps, shall be supported.
   b) *Concatenated OC-3c*. In this mode, a single channel equivalent to information payload data rate of 148.608 Mbps shall be supported.
9. **SONET OC-12**. Line rate of 622.080 Mbps, which may be used to provide channelized OC-12 or concatenated OC-12c:
   a) *Channelized OC-12*. In this mode, 4 separate OC-3 channels, each with an information payload data rate of 148.608 Mbps, shall be supported.
   b) *Concatenated OC-12c*. In this mode, a single channel equivalent to an information payload data rate of 594.432 Mbps shall be supported.
10. **SONET OC-48**. Line rate of 2.488 Gbps, which may be used to provide channelized OC-48 or concatenated OC-48c:
    a) *Channelized OC-48*. In this mode, 4 separate OC-12 channels, each with an information payload data rate of 594.432 Mbps, shall be supported.
    b) *Concatenated OC-48c*. In this mode, a single channel equivalent to an information payload data rate of 2.377728 Gbps shall be supported.
11. **SONET OC-192**. Line rate of 10 Gbps, which may be used to provide channelized OC-192 or concatenated OC-192c:
    a) *Channelized OC-192*. In this mode, 4 separate OC-48 channels, each with an information payload data rate of 2.488 Gbps, shall be supported.
    b) *Concatenated OC-192c*. In this mode, a single channel equivalent to an information payload data rate of 9.510912 Gbps shall be supported.

12. **(Optional) SONET OC-768**. Line rate of 40 Gbps, which may be used to provide channelized OC-768 or concatenated OC-768c:
    a) *Channelized OC-768*. In this mode, 4 separate OC-192 channels, each with an information payload data rate of 9.510912 Gbps, shall be supported.
    b) *Concatenated OC-768c*. In this mode, a single channel equivalent to an information payload data rate of 38.486016 Gbps shall be supported.
13. **(Optional) Subrate DS0**. Information payload data rates of 4.8, 9.6, and 19.2 Kbps.
14. **(Optional) Analog Line (4KHz)**.
15. **(Optional) Fractional T1**. Two, four, six, eight, or twelve adjacent DS0 clear channels over an interface of T1 with a line rate of 1.544 Mbps.
16. **Fractional T3**. Two adjacent T1 clear channels over an interface of T3 with a line rate of 44.736 Mbps.

C.2.1.4.2 Features

The following PLS features are mandatory unless marked optional:

ID Number	Name of Feature	Description
1	Multipoint Connection	The contractor shall allow interconnection of three or more subscriber premises as follows: Branch-Off. In this mode, all SDPs shall be treated as one shared medium and each point shall be able to autonomously send and receive data. The application will ensure master/slave mode of operation (e.g., polling scheme used in IBM 3270 mode of data communication). Drop-and-Insert. In this mode, previously specified channels of a channelized T1, T3, SONET OC-3, or SONET OC-12 service category shall be able to be dropped off and new channels shall be able to be simultaneously picked up or inserted.
2	Special Routing	The contractor shall provide different routes for PLS circuits based on the following arrangements: Transport Diversity. Between connecting POPs, the contractor shall supply two or more physically separated routes for PLS circuits. These diverse routes shall not share common telecommunications facilities or offices. The contractor shall maintain a minimum separation of 30 feet throughout all diverse routes. The government recognizes that uncompromised (i.e., adhering to the minimum separation requirements as described above) diversity may not be

ID Number	Name of Feature	Description
		available in some locations. Where uncompromised diversity is not available, the contractor shall exert best efforts to propose an acceptable arrangement along with documentation describing the compromise. Each pair of circuits that must be diverse from each other constitutes a relationship pair. For example, three circuits ordered as being diverse from each other constitute three relationship pairs, i.e., 1 and 2, 1 and 3, and 2 and 3. If diversity is not available or the compromised diversity is not acceptable to the government, it shall be negotiated on an individual case basis. Transport Avoidance. Between connecting POPs, the contractor shall supply the capability for a customer to define a geographic location or route on the network to avoid. The government recognizes that avoidance may not be available in some locations. Where avoidance is not available, the contractor shall exert best efforts to propose an acceptable arrangement along with documentation describing the reasons for the unavailability. The contractor shall establish an internal control (i.e., electronic flagging of routes) to prevent accidental dismantling of diversified/avoidance routes, especially during routine route optimization initiatives by the contractor. The contractor shall provide, within 30 calendar days of the implementation of transport diversity or avoidance, and again thereafter whenever a change is made, a graphical representation (e.g., diagrams/maps) of transport circuit routes to show where diversity or avoidance has been implemented. The contractor shall provide, at least 30 calendar days in advance of implementation, written notification to the agency (with a copy to the PMO) requesting government approval of any proposed reconfiguration of routes that were previously configured for transport diversity or avoidance. When a user selects an explicit diversity and/or avoidance, the performance level of the PLS circuit will be specified by the user at the service ordering time.

C.2.1.4.3 Interfaces

The UNIs at the SDP are mandatory unless marked optional:

UNI Type	Interface Type and Standard	Payload Data Rate	UNI Type
1	ITU-TSS V.35	Up to 1.92 Mbps	Transparent
2	EIA RS-449	Up to 1.92 Mbps	Transparent
3	EIA RS-232	Up to 19.2 Kbps	Transparent
4	EIA RS-530	Up to 1.92 Mbps	Transparent
5	T1 (with ESF) [Std: Telcordia SR-TSV-002275; ANSI T1.403}	Up to 1.536 Mbps	Transparent
6	T3 [Std: Telcordia GR-499-CORE]	Up to 43.008 Mbps	Transparent
7	E1 [Std: ITU-TSS G.702]	Up to 1.92 Mbps	Transparent
8	E3 [Std: ITU-TSS G.702]	Up to 30.72 Mbps	Transparent
9 (optional)	Optical: SONET OC-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	Transparent
10 (optional)	Electrical: SONET STS-1/EC-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	Transparent
11	SONET OC-3 (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
12	SONET OC-3c (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
13	SONET OC-12 (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
14	SONET OC-12c (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
15	SONET OC-48 (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent
16	SONET OC-48c (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent

UNI Type	Interface Type and Standard	Payload Data Rate	UNI Type
17	SONET OC-192 (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent
18	SONET OC-192c (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent
19 (Optional)	SONET OC-768 (Std: ANSI T1.105 and 106)	38.486016 Gbps	Transparent
20 (Optional)	SONET OC-768c (Std: ANSI T1.105 and 106)	38.486016 Gbps	Transparent

C.2.1.4.4 Performance Metrics

The performance levels and AQL of KPIs for PLS circuits are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability (POP-to-POP)	Routine	99.9%	≥ 99.9%	See Note 1
	Critical	99.99%	≥ 99.99%	
Availability (SDP-to-SDP)	Routine	99.9%	≥ 99.9%	
	Critical	99.99%	≥ 99.99%	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Availability:

   a) For data rates of T1 and higher, a service is considered unavailable when a PLS circuit experiences 10 consecutive severely errored seconds (SES) [Standard: Telcordia PUB GR-418-CORE]. An unavailable circuit is considered available when restoration activities have been completed and 30 consecutive minutes have passed without any errored seconds to account for stability and proving period. However, if there is no error second encountered during the proving period of 30 minutes, this will not be counted towards the circuit unavailable time.

b) For data rates lower than T1, cumulative outage time is calculated based on trouble ticket data.

c) PLS availability is calculated as a percentage of the total reporting interval time that PLS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100 .$$

Critical level of Service for availability only applies to T1 and above data rates.

2. Refer to Section G.8.2 for definition and how to measure.

C.2.1.5 Synchronous Optical Network Service

C.2.1.5.1 Service Description

Synchronous Optical Network Service (SONETS) is the U.S. standard for fiber optic synchronous transmission rates from 51.84 Mbps to beyond 40 Gbps while Synchronous Digital Hierarchy (SDH) is the International Telecommunications Union version, which begins at 155 Mbps. SONET transport is highly reliable and provides proactive performance monitoring that prevents single and multiple failures and further enables self-healing functions and robust network management.

C.2.1.5.1.1 Functional Definition

SONETS supports a wide range of digital signals with different capacities, and its interworking capability enables seamless communications between devices that support dissimilar protocols such as IP, Frame Relay, and ATM.

C.2.1.5.1.2 Standards

SONETS Service shall comply with the following standards unless marked optional:

1. Telcordia Technologies:

   a) (Optional) GR-1031 OTGR Section 15.6: Operations Interfaces Using OSI Tools: Test Access Management(10/97)

   b) (Optional) GR-1042 Generic Requirements for Operations Interfaces Using OSI Tools - Information Model Overview: Synchronous Optical Network (SONET) Transport Information Model (12/98)

c) (Optional) GR-1042-IMD Generic Requirements for Operations Interfaces Using OSI Tools - Information Model Details: Synchronous Optical Network (SONET) Transport Information Model (12/98)

d) (Optional) GR-1110 Broadband Switching System (BSS) Generic Requirements (12/00)

e) GR-1209 Generic Requirements for Passive Optical Components (03/01)

f) GR-1230 SONET Bi-Directional Line-Switched Ring Equipment Generic Criteria (12/98)

g) GR-1250 Generic Requirements for Synchronous Optical Network (SONET) File Transfer (12/99)

h) (Optional) GR-1345 Framework Generic Requirements for Element Manager (EM) Applications for SONET Subnetworks (12/00)

i) GR-1365 SONET Private Line Service Interface Generic Criteria for End Users (12/94)

j) GR-1374 SONET Inter-Carrier Interface Physical Layer Generic Criteria For Carriers (12/94)

k) GR-1400 SONET Dual-Fed Unidirectional Path Switched Ring (UPSR) Equipment Generic Criteria (01/99)

l) GR-199 OTGR Section 12.2: Operations Application Messages - Memory Administration Messages (08/02)

m) GR-253 Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria (09/00)

n) (Optional) GR-2837 ATM Virtual Path Ring Functionality in SONET - Generic Criteria (02/98)

o) (Optional) GR-2842 ATM Service Access Multiplexer Generic Requirements (11/96)

p) (Optional) GR-2875 Generic Requirements for Digital Interface Systems (05/96)

q) (Optional) GR-2891 SONET ATM Virtual Path Digital Cross-Connect Systems - Generic Criteria (12/98)

r) (Optional) GR-2899 Generic Criteria for SONET Two-Channel (1310/1550-NM) Wavelength Division Multiplexed Systems (09/95)

s) (Optional) GR-2900 SONET Asymmetric Multiples Functional Criteria (09/95)

t) GR-2918 DWDM Network Transport Systems with Digital Tributaries for Use in Metropolitan Area Applications: Common Generic Criteria (01/03)

u) GR-2950 Information Model for SONET Digital Cross-Connect Systems (DCSS) (02/99)

v) (Optional) GR-2954 Transport Performance Management Based on the TMN Architecture (12/97)

w) (Optional) GR-2955 Generic Requirements for Hybrid SONET/ATM Element Management Systems (EMSS) (11/98)

x) GR-2979 Generic Requirements for Optical Add-Drop Multiplexers (OADMs) and Optical Terminal Multiplexers (OTMs) (12/01)

y) (Optional) GR-2980 Generic Criteria for ATM Layer Protection Switching Mechanism (12/98)

z) GR-2996 Generic Criteria for SONET Digital Cross-Connect Systems (01/99)

å) (Optional) GR-3000 Generic Requirements for SONET Element Management Systems (EMSs) (11/99)GR-3001 Generic Requirements for SONET Network Management Systems (NMS's) (12/99)

ä) (Optional) GR-3004 Generic Requirements for the Operations Interface Between Hybrid SONET/ATM Element Management Systems and Network Management Systems (02/99)

ö) GR-3008 OTGR Section 6.9: Network Maintenance: Access and Testing - SONET STS-1 and SUB-STS-1 TSC/RTU and DTAU Functional Requirements (12/98)

aa) GR-303 Integrated Digital Loop Carrier System Generic Requirements, Objectives, and Interface (12/00)

bb) (Optional) GR-3101 Generic Requirements for Asynchronous Transfer Mode (ATM) Element Management Systems (EMSs) (08/00)

cc) (Optional) GR-3102 Generic Requirements for Asynchronous Transfer Mode (ATM) Network Management Systems (10/00)

dd) (Optional) GR-376 Generic Operations Interfaces Using OSI Tools: Network Data Collection (12/98)

ee) GR-436 Digital Network Synchronization Plan (06/94)

ff) GR-496 SONET Add-Drop Multiplexer (SONET ADM) Generic Criteria (12/98)

gg) GR-499 Transport Systems Generic Requirements (TSGR): Common Requirements (12/98)

hh) GR-782 SONET Digital Switch Trunk Interface Criteria (06/00)

ii) (Optional) GR-826 OTGR Section 10.2: User Interface Generic Requirements For Supporting Network Element Operations (06/94)

jj) GR-834 Network Maintenance: Access and Testing Messages (06/00)

kk) (Optional) GR-836 Generic Operations Interfaces Using OSI Tools: Information Model Overview: Transport Configuration and Surveillance For Network Elements

2. ANSI Standards:

    a) ANSI T1.105: SONET - Basic Description including Multiplex Structure, Rates and Formats
    b) ANSI T1.105.01: SONET - Automatic Protection Switching
    c) ANSI T1.105.02: SONET - Payload Mappings
    d) ANSI T1.105.03: SONET - Jitter at Network Interfaces
    e) ANSI T1.105.03a: SONET - Jitter at Network Interfaces - DS1 Supplement
    f) ANSI T1.105.03b: SONET - Jitter at Network Interfaces - DS3 Wander Supplement
    g) ANSI T1.105.04: SONET - Data Communication Channel Protocol and Architectures
    h) ANSI T1.105.05: SONET - Tandem Connections Maintenance
    i) ANSI T1.105.06: SONET - Physical Layer Specifications
    j) ANSI T1.105.07: SONET - Sub-STS-1 Interface Rates and Formats Specification
    k) ANSI T1.105.09: SONET - Network Element Timing and Synchronization
    l) ANSI T1.119: SONET - Operations, Administration, Maintenance, and Provisioning (OAM&P) – Communications
    m) ANSI T1.119.01: SONET: OAM&P Communications Protection Switching Fragment

3. ITU-T Standards:

    a) Physical Interfaces:
        i. G.703 (10/98)
        ii. G.957 (06/99)
        iii. G.692 (10/98)
        iv. K.20 (05/98)
        v. G.691 (04/00)
    b) Network Architecture:
        i. G.805 (11/95), (03/00)
        ii. G.803 (06/97), (03/00)
        iii. I.322 (02/99)
    c) Structures & Mappings:
        i. G.704 (10/98)
        ii. G.707 (10/00) - Amendment 1
        iii. G.7041 (10/01) Generic Framing Procedure

  iv. G.7042 (10/01) LCAS
  v. G.708 (10/98)
  vi. G.832 (10/98)

d) Equipment Functional Characteristics:
  i. G.664 (06/99)
  ii. G.781 (06/99)
  iii. G.783 (10/00)
  iv. G.958 (01/94)
  v. G.705 (04/00)
  vi. G.806 (04/0)

e) Laser Safety:
  i. G.664 (06/99)

f) Transmission Protection:
  i. G.841 (10/98), (08/02)
  ii. G.842 (04/97)
  iii. G.808.1 (2003)
  iv. M.2102 (03/00)

g) Equipment Protection:
  i. M.3100 Amendment

h) Equipment Management:
  i. G.784 (06/99)

i) Information Model:
  i. G.773 (03/93)
  ii. G.774 (09/92), (11/96), (04/00)
  iii. G.774.01 (11/94), (11/96), (04/00)
  iv. G.774.02 (11/94), (11/96), (04/00)
  v. G.774.03 (11/94), (11/96), (04/00)
  vi. G.774.04 (07/95), (11/96), (04/00)
  vii. G.774.05 (07/95), (11/96), (04/00)
  viii. G.774.06 (04/00)
  ix. G.774.07 (11/96), (04/00)
  x. G.774.08 (04/00)
  xi. G.774.09 (04/00)
  xii. G.774.10 (04/00)

j) Network Management:

  i. G.831 (08/96), (03/97)
  ii. T.50 (09/92)
  iii. G.85x.y (11/96)

k) Error Performance (network level view):
  i. G.826 (02/99)
  ii. G.827 (02/00)
  iii. G.827.1 (11/00)
  iv. G.828 (02/00)
  v. G.829 (02/00)
  vi. M.2101 (02/00)
  vii. M.2101.1 (04/97)
  viii. M.2102 (02/00)
  ix. M.2110 (04/97)
  x. M.2120 (04/97), (02/00)
  xi. M.2130 (02/00
  xii. M.2140 (02/00)

l) Error Performance (equipment level view):
  i. G.783 (10/00)
  ii. G.784 (06/99)

m) Jitter and Wander Performance:
  i. G.813 (08/96)
  ii. G.822 (1988)
  iii. G.823 (03/93), (03/00)
  iv. G.824 (03/93), (03/00)
  v. G.825 (03/93), (02/99)
  vi. G.783 (10/00), (04/97), (03/99), (06/98)

n) Leased Lines:
  i. M.13sdh (02/00)

o) Synchronization (Clocks and Network Architecture:
  i. G.803 (06/97), (02/99)
  ii. G.810 (08/96)
  iii. G.811 (09/97)
  iv. G.812 (06/98)
  v. G.813 (08/96)

p) Test Signals:

i. O.150

ii. O.181

4. Institute of Electrical and Electronics Engineers, Inc. (IEEE):
   a) IEEE 802.3 (as updated from time to time by IEEE), 1Gbps LAN PHY, 10Gbps LAN PHY, 10Gbps WAN PHY
   b) (Optional) IEEE 802.3ae (as updated from time to time by IEEE), 10Gbit Ethernet
   c) 802.17, Resilient Packet Rings (RPR) – in progress
   d) 802.1ah, Ethernet First Mile – in progress
5. Optical Internetworking Forum (OIF):
   a) User to Network Interface version 1.0, OIF-UNI-01.0
6. All new versions, amendments, and modifications to the above documents and standards

C.2.1.5.1.3 Connectivity

SONETS services shall connect to and interoperate with:

1. Government-specified terminations (e.g., SDP-to-SDP, POP-to-POP)
2. All other networks including other EIS contractors' networks where industry standards are used

C.2.1.5.1.4 Technical Capabilities

The following SONETS capabilities are mandatory unless marked optional:

1. Geographical Coverage. The contractor shall comply with the following requirements:
   a) (Optional) The contractor shall support OCONUS and Non-Domestic SONETS
   b) The contractor shall support Continental US (CONUS) Domestic SONETS
   c) The contractor shall support SONETS in the Metro area
2. (Optional) Gateway functionality (SONET to SDH and SDH to SONET conversion) as needed by agency.
3. The contractor shall support one or more of the following Network Topologies:
   a) Linear topologies such as Point-to-Point
   b) Ring topology
   c) Mesh topology

4. The contractor shall support one or more of the following protection methods:
    a) On the Tributary Side the contractor shall support:
        i. Automatic Protection Switching (APS) 1:N, where N ≤ 14
        ii. APS 1+1
        iii. Unprotected
    b) On the Network Side the contractor shall support:
        i. Unprotected
        ii. Mesh Protection
        iii. Unidirectional Path Switched Ring (UPSR)
        iv. Bidirectional Line Switched Ring (BLSR)
        v. (Optional) Bidirectional Path Switched Ring (BPSR) or equivalent
        vi. 1+1
5. Transmux Capability (interconnects high bandwidth interface at one agency location to lower bandwidth interface at another agency location):
    a) (Optional) DS3/STS1 transmuxed to DS1 shall be supported
    b) OC3 transmuxed to DS3/STS1 shall be supported
    c) OC12 transmuxed to OC3/DS3/STS1 shall be supported
    d) OC48 transmuxed to OC12/OC3/DS3/STS1 shall be supported
    e) (Optional) OC192 transmuxed to OC48/OC12/OC3/DS3/STS1 shall be supported
6. (Optional) The following concatenation methods shall be included in SONETS:
    a) Standard Concatenation. SONET specifications in GR-253 include standard concatenation, which allows OC-N signals to be grouped in multiples of 3 STS-1s and treated as single entities. The following standard concatenated rates shall be supported:
        i. STS-12c shall be supported
        ii. STS-48c shall be supported
        iii. (Optional) STS-192c shall be supported
        iv. (Optional) STS-768c shall be supported
    b) Virtual Concatenation. The following standard rates shall be available for agency procurement: (Optional)
        i. VT-1.5-7v for 10 Mbps Ethernet Connections shall be supported
        ii. VT-2.0-5v for 10 Mbps Ethernet Connections shall be supported
        iii. STS-1-2v for 100 Mbps Fast Ethernet Connections shall be supported
        iv. STS-1-21v for 1Gbps Ethernet Connections shall be supported

   v. STS-3c-7v for 1Gbps Ethernet Connections shall be supported

  c) The contractor shall support the following:

   i. High order concatenation – shall support STS-1/3c-*X*v SPE, *X* = 1 up to 256 rates/entities

   ii. Low order concatenation – shall support X VTn SPEs (n=1.5, 2, 3, 6) rates/entities

7. Performance Monitoring: The contractor shall support the Performance Monitoring parameters specified by GR-253. Monitoring of parameters shall be for each individual minute and recorded in registers of 15 minutes. The last eight 15-minute registers shall be archived and made accessible to the agency. The contractor shall store all measurements for the past 24 hours in a register. The following parameters shall be monitored, and measured:

   a) Errored Seconds. An Errored Second is any one-second interval containing at least one error. Errored Seconds shall be counted as 1-second intervals containing at least 1 error. The contractor shall measure performance based on percent of error seconds, which is calculated as 100 times the ratio of error seconds to total seconds in the available time during a fixed measurement period (24 hours). For all EIS users, the percentage of Errored Seconds shall be less than 0.25% during the measurement period. It is AQL to observe Errored Seconds during 1.8 minutes per month.

   b) Severely Errored Seconds (SES). A SES is 1-second period with a bit error rate per second of 10^{-3} or worse for DS-1 and DS-3 signals. SES for STS-n signals, is 1-second period that contains 30 percent or greater errored blocks or at least one severely disturbed period. A severely disturbed period occurs when all contiguous blocks are affected by a high bit error density over a period of 1 millisecond. The contractor shall measure performance based on percent of SES, which is calculated as 100 times the ratio of SES to total seconds in available time during a fixed measurement period (24 hours). For all EIS users, the percentage of SES shall be less than 0.035% during the measurement period. It is AQL to observe SES during 15.12 seconds per month.

8. Synchronization and Timing Methods. The contractor shall support the following:

   a) External Timing

   b) Line Timing

9. Reserved

10. (Optional) Next Generation SONET shall be supported.

11. The contractor's network shall support all of the following:

i. Generic Framing Procedure, shall include:
    1. Frame Mapped Generic Framing Procedure
    2. Transparent Generic Framing Procedure
ii. Link Adjustment Capacity Scheme (LCAS) shall be supported to provide Virtual Concatenation as defined by ANSI T1.105 and G.707
iii. (Optional) Virtual Concatenation shall be supported.

12. (Optional) Data Communications Channel (DCC) – The contractor shall provide the agency with the ability to establish communication between its edge devices.

13. (Optional) Integrated Control Plane (i.e. ASON based, GMPLS) – Support of an integrated, intelligent control plane in order to speed up activation service times, provide control to agencies to the contracted infrastructure and achieve inter- and intra-contractor interoperability when required.

C.2.1.5.2 Features

The following SONETS Service features are mandatory unless marked optional:

Service Features ID Number	Name of Feature	Description
1 (optional)	Channelization	The contractor shall support SONET interfaces to the CPE to seamlessly interface with the contractor's SONET network for data transport. The following channelized arrangements shall be supported as a minimum: 1. STS-1 payload with VT1.5, VT2 2. STS-1, STS-1 payload, VT1.5, VT2, STS-3c 3. VC-11(DS1), VC-12 (E1), VC-3 (DS3, E3, other) 4. VC-4, VC-3, VC-11, VC-12 5. Down to STS-1 (E3, other) 6. STM-1, VC-11 (DS1), VC-12 (E1), VC-3 (DS3, E3, other), VC-4
2 (Optional)	DS1 Rate Synchronization Service	The contractor shall provide the agency with this feature to allow agency's Stratum 2 or Stratum 3 clocks at its locations to synchronize to a Stratum 1 clock at the contractor's location. The DS1 to be used for

Service Features ID Number	Name of Feature	Description
		synchronization shall be delivered through the following methods: 1. External Timing
3	SONET Performance	All SONET services contracted by the agencies shall comply with the following performance indicators and with the Performance Metrics included in Section C.2.1.5.4: 1. Jitter -- as specified in GR-253 - Jitter measurement is performed over a 60-second interval with band pass filters having frequencies cut off at 10 KHz and 4 KHz, a fall of 20db/decade, and a low-pass cut off frequency of at least 80 KHz. The contractor shall ensure these specifications are met at the SDPs. 2. Restoration Time -- as specified by GR-253 for Automatic Protection Switching and by GR-1230, Section 6.1.1, re-routing of the traffic shall be performed to restore the SONETS (over redundant path) before the failure is repaired. The contractor shall reconfigure affected services for Rings < 1200 KM as follows: a) For Routine Users, in less than 100 ms, when preemption of extra traffic is required. b) For Critical Users, in less than 60 ms including detection time (10ms).
4	Equipment Protection – Network Side	The contractor shall provide protection to the client interfaces at the SDP, where the protection channel is bridged to the failed working channel.
5	Framing for Electrical Interfaces	The following framing formats for electrical interfaces shall be supported: 1. (Optional) M-frame with M23 Multiplexing format. 2. M-frame with C-parity.

Service Features ID Number	Name of Feature	Description
		3. (Optional) Super Frame (SF) Format. 4. (Optional) Bipolar Alternate Mark Inversion. 5. Binary, 8 zero substitution line code. 6. (Optional) Non-ANSI SF. 7. ANSI Extended Superframe (ESF) (ANSI T1403, 1995). 8. (Optional) Non-ASNI ESF (AT&T PUB 54016).
6	Geographic Diverse Protection	The feature shall ensure a minimum separation of 25 feet between the diverse circuits end-to-end. In addition, the contractor shall ensure that the diverse circuits are specifically flagged to prevent disconnection during network grooming activity.
7	Local and Remote Node Multiplexing	This feature shall enable the multiplexing of different low-speed circuits onto a high-speed SONET signal, such as SONET OC3 and OC12.

C.2.1.5.3 Interfaces

The UNIs at the SDP are mandatory unless marked optional.

UNI Type	Interface Type	Standard (as updated from time to time by the applicable governing entity)	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling/Protocol Type/Granularity
1	Optical	IEEE 802.3z	1310 nm	1.25Gbps	Gigabit Ethernet
2	Optical	IEEE 802.3z	850 nm	1.25Gbps	Gigabit Ethernet
3	Optical	IEEE 802.3	1310 nm	125 Mbps	Fast Ethernet
4	Optical	GR-253, ITU-T G.707	1310 nm	155 Mbps	SONET or SDH
5	Optical	GR-253, ITU-G.707	1310 nm	155 Mbps	SONET or SDH Concatenated
6	Optical	GR-253, ITU-G.707	1310 nm	622 Mbps	SONET or SDH

UNI Type	Interface Type	Standard (as updated from time to time by the applicable governing entity)	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling/Protocol Type/Granularity
7	Optical	GR-253, ITU-G.707	1310 nm	622 Mbps	SONET or SDH Concatenated
8	Optical	GR-253, ITU-T G.707	1310 nm	622 Mbps	SONET Channelized
9 (Optional)	Optical	GR-253	1310 nm	155 Mbps	ATM over SONET
10 (Optional)	Optical	GR-253	1310 nm	622 Mbps	ATM over SONET
11	Optical	GR-253, ITU-T G.707	1310 nm	2.5Gpbs	SONET or SDH
12	Optical	GR-253, ITU-T G.707	1310 nm	2.5Gbps	SONET or SDH Concatenated
13 (Optional)	Optical	GR-253, ITU-T G.707	1310 nm	10Gbps	SONET or SDH
14	Electrical	ANSI T1	N/A	1.544 Kbps	DS1
15	Electrical	ANSI T1	N/A	45 Mbps	DS3
16	Electrical	ANSI T1	N/A	45 Mbps	STS-1
17	Electrical	ANSI T1	N/A	DS1	DS0, Nx64 Kbps
18	Electrical	ANSI T1	N/A	DS3	DS3, Nx1.544Mbps, DS1
19	Electrical	ANSI T1	N/A	E1	Nx64 Kbps
20	Electrical	ANSI T1	N/A	E3	E1, Nx64 Kbps, DS0
21 (Optional)	Optical	GR-253, ANSI T1.105	1300 nm	OC-1	SONET STS-1 payload, VT1.5, VT2
22 (Optional)	Optical	GR-253, ANSI T1.105	1300 nm	OC-3 155 Mbps	SONET STS-1, STS-1 payload, VT1.5, VT2
23	Optical	GR-253, ANSI T1.105	1300 nm	OC-3c 155 Mbps	SONET STS-3c
24	Optical	G.707	1300 nm	STM-1 155 Mbps	SDH VC-11(DS1), VC-12 (E1), VC-3 (DS3, E3, other)
25	Optical	G.707	1300 nm	STM-1c 155 Mbps	SDH VC-4, VC-3, VC-11, VC-12

UNI Type	Interface Type	Standard (as updated from time to time by the applicable governing entity)	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling/Protocol Type/Granularity
26 (Optional)	Optical	GR-253, ANSI T1.105	1300 nm	OC-12 622 Mbps	SONET Down to VT1.5 (DS1), VT2 (E1), STS-1 (DS3, E3, other), STS-3c
27	Optical	GR-253, ANSI T1.105	1300 nm	OC-12c 622 Mbps	SONET STS-12c
28	Optical	ITU-T G.707	1300 nm	STM-4	SDH STM-1, VC-11 (DS1), VC-12 (E1), VC-3 (DS3, E3, other), VC-4
29	Optical	ITU- G.707	1300 nm	STM-4c	VC-4-4c
30 (Optional)	Optical	OIF- VSR4-01.0	850 nm	OC-192	VSR4-01 OC-192 (12 fibers)
31 (Optional)	Optical	OIF-VSR4-03.0	1310 nm	OC-192	VSR4-02 OC-192 (1 fiber)
32 (Optional)	Optical	OIF-VSR4-03.0	850 nm	OC-192	VSR4-03 OC-192 (4 fibers)
33 (Optional)	Optical	OIF-VSR4-04.0	850 nm	OC-192	VSR4-04 OC-192 (1 fiber)
34 (Optional)	Optical	OIF-VSR4-05.0	1310 nm	OC-192	VSR4-05 OC-192
35 (Optional)	Optical	OIF-VSR5-01	850 nm	OC-768	VSR5-01 OC-768
36	Electrical	GR-253, ANSI T1.105	850 nm	STS-1/EC-1 51.84 Mbps	SONET/STS-1, VT1.5 mapping
37 (Optional)	Optical	GR-253	1550 nm	2.5 Gbps	SONET or SDH
38 (Optional)	Optical	GR-253	1550 nm	10 Gbps	SONET or SDH

C.2.1.5.4 Performance

The contractor shall support In-Service Monitoring (ISM) at the SONET Layer and shall not rely on performance observed and measured at higher layers of the network.

The performance levels and AQL of KPIs for SONET Service are mandatory unless marked optional.

Key Performance Indicators	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Av(SONETS) (SDP-to-SDP)	Routine	99.8%	≥ 99.8%	In Service Monitoring See Note 1
	Critical	99.999%	≥ 99.999%	
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. SONETS availability shall be measured in-service and on an end-to-end basis. COT (HR) shall be calculated based on Errored Seconds and/or SES as defined by GR-253, G.826 through G.829 and shall be expressed in hours. Availability is computed by the standard formula:

$$Av(SONETS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100 .$$

C.2.1.6 Dark Fiber Service

C.2.1.6.1 Service Description

Dark fiber is optical fiber infrastructure (cabling and repeaters) in which the light is provided by the customer rather than the carrier. The simplest Dark Fiber Service (DFS) is a point-to-point connection between two locations. Other configurations enable agencies to interconnect any number of selected locations.

C.2.1.6.1.1 Functional Definition

DFS is acquired as a facility which allows the agency the unconditional right to use a fiber route, which provides capacity such as a fiber pair in a fiber-optic cable or the entire fiber-optic cable. Agencies which acquire dark fiber may either provide their own optronics equipment or lease it from the contractor. Agencies which prefer not to design, implement, and manage their own optical networks can use Managed Network Service (MNS) as a Managed Dark Fiber Service to design, implement, and manage optical networks to meet their unique mission requirements.

C.2.1.6.1.2 Standards

DFS shall comply with the following standards:

1. Electronic Industry Alliance/Telecommunications Industry Association (EIA/TIA):

a) EIA/TIA-559, Single Mode Fiber Optic System Transmission Design.

b) Optical Fiber System Test Procedures (OFSTPs) including:

   i. OFSTP-2, Effective Transmitter Output Power Coupled into Single Mode Fiber Optic Cable
   ii. OFSTP-3, Fiber Optic Terminal Receiver Sensitivity and Maximum Receiver Input
   iii. OFSTP-7, Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant
   iv. OFSTP-14, Measurement of Optical Power Loss of Installed Multi-Mode Fiber Cable Plant
   v. OFSTP-10, Measurement of Dispersion Power Penalty in Single Mode Systems
   vi. OFSTP-11, Measurement of Single Reflection Power Penalty for Fiber Optic Terminal Equipment

2. Telcordia Standards:

   a) GR-20-CORE, Generic Requirements for Optical Fiber and Optical Fiber Cable
   b) GR-63-CORE, Network Equipment-Building System (NEBS), Generic Equipment Requirements
   c) GR-253-CORE, Synchronous Optical Network (SONET) Transport Systems: Common Criteria Physical Layer
   d) GR-326-CORE, Generic Requirements for Single Mode Connectors and Jumper Assemblies

3. American National Standards Institute (ANSI):

   a) ANSI Z136.2-1998, American National Standard for the Safe Use of Optical Fiber Communications Systems Utilizing Laser Diode and LED Sources

4. International Electrotechnical Commission (IEC):

   a) IEC 60825-1,Safety of Laser Products, Part 1: Equipment Classification, Requirements and User’s Guide, Consolidated Edition – International Restrictions
   b) IEC 60825-2, Safety of Laser Products, Part 2: Safety of Optical Fiber Communications Systems (OFCS) – International Restrictions.

5. Code of Federal Regulations (CFR):

   a) 21 CFR 1040, Performance Standard for Laser Products

6. International Telecommunications Union (ITU-T):

   a) ITU-T G.655 (10/2000)

   b) ITU-T G.652 (10/2000)
   c) ITU-T G.694.1
   d) ITU-T K.25 (02/2000)
   e) ITU-T L.35 (10/1998)

7. Regulations and Permits – The contractor shall be responsible for all permits, easements, and rights of way, to include Host Nation agreements/approvals. The contractor shall be responsible for complying with local government regulations. If obstacles are found during the process that will affect agency’s schedule negatively, the contractor shall coordinate solutions with the government.
8. All new versions, amendments, and modifications to the above documents and standards.

C.2.1.6.1.3 Connectivity

DFS shall connect to and interoperate with:

1. Inter-agency or intra-agency LANs within the same vicinity. This service shall enable an agency to interconnect via inter-agency or intra-agency LAN to selected locations situated within the same metro area (i.e., city). Examples of supported configurations are outlined in Section C.2.1.6.1.4 #2.
2. The contractor’s Long Haul or Metro networks. This service shall enable an agency to connect its locations(s) to the nearest contractor’s wire center, LEC wire center, Hut, IXC POP, or CLEC collocation facility as applicable.
3. Redundant paths to support agency's transport infrastructure, thereby enhancing service reliability.
4. The contractor shall terminate fiber(s) in the existing Fiber Distribution Panel (FDP) or the FDP specified by the agency using connectors specified by industry’s standards for:
   a) Multi-tenant buildings
   b) Single tenant buildings

C.2.1.6.1.4 Technical Capabilities

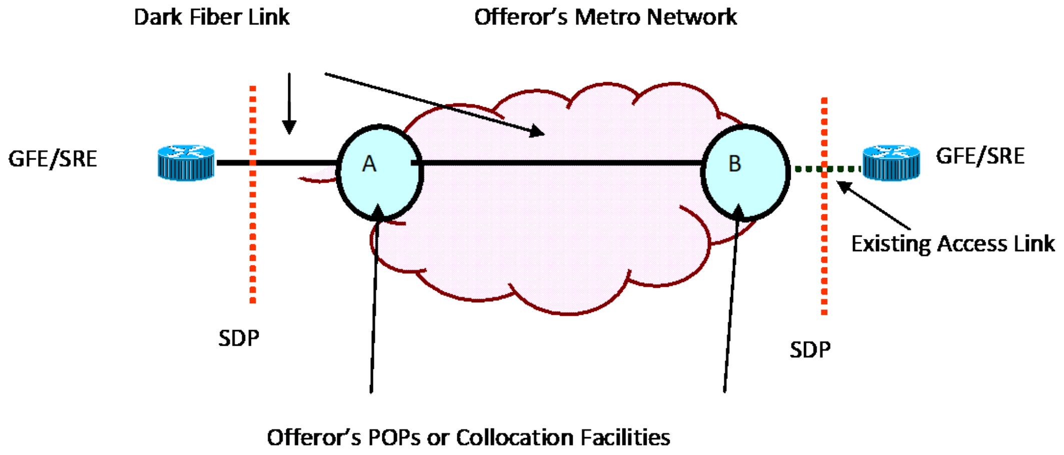
The following DFS capabilities are mandatory unless marked optional:

1. Geographical Coverage. The contractor shall specify the coverage of its DFS in the following regions when required as part of a TO:
   a) CONUS
   b) (Optional) Non-domestic

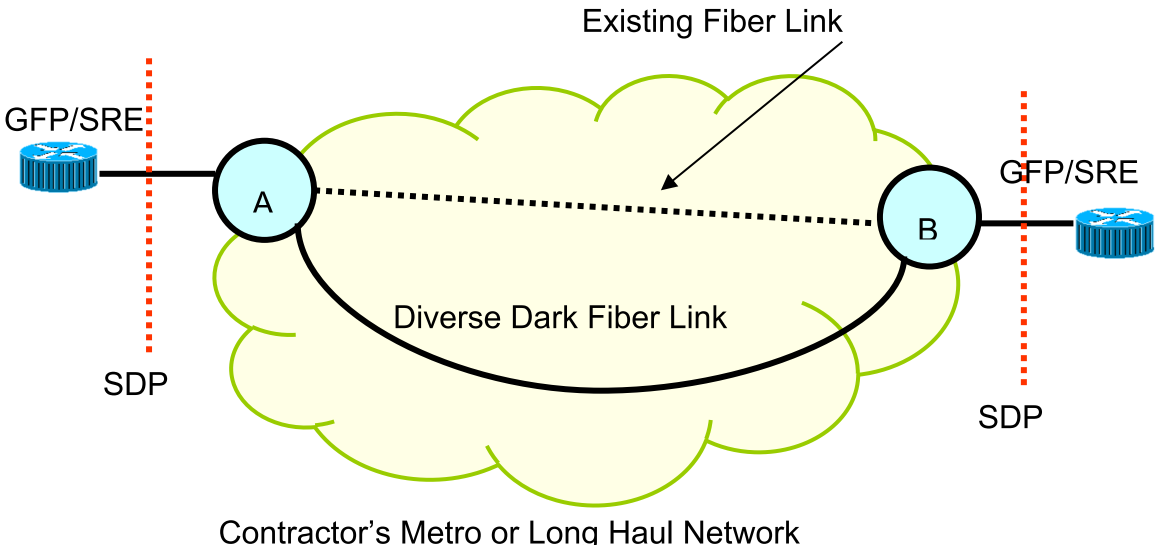
c) (Optional) OCONUS

2. Configuration Alternatives. The contractor shall support the network topologies outlined as follows:

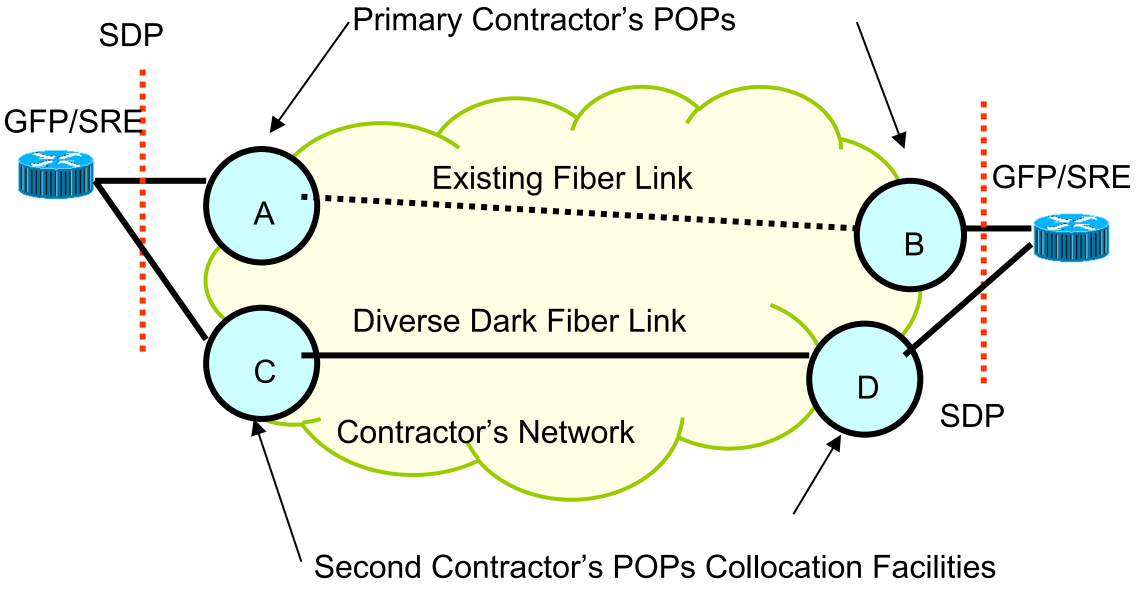
   a) Point-to-point. This configuration connects any two points in the contractor's network. The figure below depicts two agency locations in a metro area connected by a dark fiber link from POP to POP.



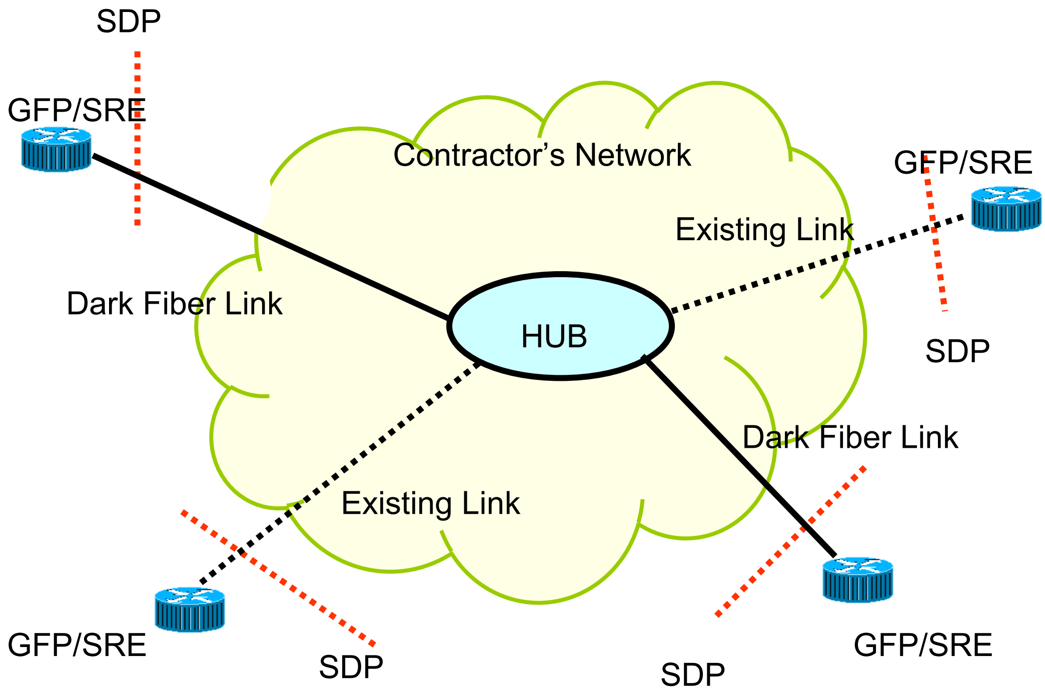
   b) Route Diversity Ring/Single Drops. This configuration is possible when the terminating equipment provides equipment and/or line protection schemes. The figure below shows that two diverse paths are available on the network to prevent service interruptions if either fiber path is damaged.



c) Route Diversity Ring/Dual Drops. This configuration is possible when two diverse paths are available end-to-end to prevent service interruptions caused by a failure in either path. The diverse path can be purchased from the same contractor and delivered to two different POPs or from a second contractor. The figure below shows that an agency has built an alternate route for protection (path C-D) using a second contractor's POPs or collocation facilities where the agency has placed its optronics.



d) Star Configuration. This configuration allows an agency to have a single location that functions as a hub that provides connectivity to other agency locations. The figure below depicts a point-to-point configuration.



Hybrid Configuration. The preceding configurations can be combined to yield a custom-tailored solution.

1. Fiber Service Delivery Point (FSDP). The contractor shall support the SDP at either the fiber patch panel where the fibers terminate at a government location or the collocation facility where the agency has installed its optronics, as required by the agency. The contractor shall meet the following conditions when delivering DFS to an agency:

   a) Optical Fiber. The fiber shall meet the standards specified in Section C.2.1.6.1.2. The contractor shall provide the number of fiber strands to be delivered at the FSDP as specified by the agency.

2. Ducting. The contractor shall provide the number of ducts between connecting locations and the number of fiber strands running in each duct as specified by the agency.

3. (Optional) Future Growth. The contractor shall include an additional duct running in parallel to the working duct(s) to provide room for anticipated growth.

4. Channel Count:

   a) Deployed fibers shall be capable of supporting a minimum of 80 DWDM wavelengths or user data with spacing as specified in ITU-T G.694.1.

   b) Deployed fibers shall be capable of operating in the "C", ”S” and “L” bands.

5. Gateways. The contractor shall provide the ability to add and drop traffic via gateway locations (nodes A, B, C, and D in the Configuration Options diagrams above are examples of gateways). The contractor shall fulfill the following requirements and provide updates on improvements or expansions throughout the life of the contract:

    a) Gateway locations shall be equipped with backup power capability and shall operate for at least 8 hours without interruption
    b) Lock cabinet spaces shall be provided
    c) 24x7 access to the gateway locations shall be provided to authorized personnel
    d) Gateway locations shall be equipped with surveillance and highly secured systems
    e) The contractor shall indicate if gateway expansion is possible
    f) The contractor shall indicate if gateway locations are monitored remotely
    g) Environmental monitoring shall be supported

6. Service Components. DFS service components shall include the following:

    a) Trunks. Trunks are main fiber cables that may carry hundreds of fiber strands, which may be shared and owned by a variety of contractors, government agencies, universities, etc.
    b) Laterals. Laterals are fiber cables from the agency's premises to the nearest splice point on the cable trunk. Their length may vary from a few meters to several kilometers.
    c) Building Entrances. Facilities within the agency's premises for the termination of fibers, i.e., fiber panel terminations.

C.2.1.6.2 Features

The following DFS features are mandatory unless marked optional.

ID Number	Name of Feature	Description
1	Colocation Service	The contractor shall provide the ability to add/drop traffic (gateways) and to regenerate and amplify traffic where needed.
2 (Optional)	Duct	The contractor shall support the number of ducts (conduits) as specified by the agency that shall be included in the service.

ID Number	Name of Feature	Description
3 (Optional)	Dark Fiber Local Loop	The contractor shall provide dark fiber connection between the agency's location and the contractor's wire center or outside plant (hut or regeneration location).
4 (Optional)	Diverse Route Single Drop	The contractor shall ensure that two diverse paths are available on the network to prevent service interruptions if a fiber on either of two paths is damaged. A Single Add/Drop location/network element shall be used in this arrangement with automatic protection switching capabilities.
5 (Optional)	Diverse Route Dual Drop	The contractor shall provide two diverse paths end-to-end to prevent service interruptions caused by a failure either in the contractor's network or at the drop's path. A second contractor shall provide the diverse route should the agency requires full diversity for protection unless the working link provider is able to do so.
6 (Optional)	Inter-city Connectivity	The contractor shall support a dark fiber connection between agency's locations in metro areas in the Continental US as well as outside the Continental US.
7 (Optional)	Multiple Duct	The contractor shall be able to upgrade to multiple ducts (conduits).
8	Splicing	The contractor shall support joining two or more lengths of optical fiber cables by way of either fusion or mechanical splicing.
9	Off-net laterals	The contractor shall provide fiber cables from the agency's premises to the nearest splice point on the cable trunk. They shall be funded by the agency and their length may vary from a few meters to several kilometers.

C.2.1.6.3 Interfaces

The interfaces for this service are the fiber terminations at the FSDP. The contractor shall identify the fiber connectors that are supported.

C.2.1.6.4 Performance Metrics

The performance levels and AQL of KPIs for DFS are mandatory unless marked optional:

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Attenuation Coefficient SMF (1550 nm)	Routine	0.25 dB/km	≤ 0.25 dB/km at all times	See Note 1
Attenuation Coefficient SMF (1310 nm)	Routine	0.35 dB/km	≤ 0.35 dB/km at all times	
Attenuation Coefficient MMF 850 nm (50/125 µm)	Routine	2.35 dB/km	≤ 2.35 dB/km at all times	
Attenuation Coefficient MMF 1300 nm (50/125 µm)	Routine	0.35 dB/km	≤ 0.35 dB/km at all times	
Polarization Mode Dispersion (PMD) at 1550 nm (Inter-City Networks)	Routine	May be specified in TO	May be specified in TO	See Note 2
Polarization Mode Dispersion (PMD) (Intra-City Networks)	Routine	May be specified in TO	May be specified in TO	
Chromatic Dispersion at 1550nm	Routine	May be specified in TO	May be specified in TO	See Note 3
Reflectance Events (all events)	Routine	Less than 40 dB	≤ 40 dB at all times	See Note 4
Connectors Loss SMF	Routine	0.1 to 0.2 dB	≤ 0.2 dB at all times	

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Fusion Splicing Loss SMF	Routine	0.05 dB	≤ 0.05 dB at all times	
End-to-End Attenuation	See Note 5			
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 6
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Attenuation coefficient is the attenuation per unit length with a maximum value at one or more wavelengths. In this case, wavelengths are from 1310nm to 1550nm.
2. Polarization Mode Dispersion (PMD) is the term that describes the relationship between polarization and group delay.
3. Chromatic dispersion measurements characterize how the velocity of propagation in fiber or components changes with wavelength.
4. Reflection measurements are done using an optical time-domain reflectometer (OTDR).
5. End-to-End Attenuation
    a. On Single Mode Fibers (SMF), end-to-end attenuation measurements shall be tested in both directions of transmission at the 1310 nm and 1550 nm wavelengths using an industry-accepted laser source and power meter.
    b. On Multi Mode Fibers (MMF), end-to-end attenuation measurements shall be tested in both directions of transmission at the 850 nm and 1300 nm wavelengths.
    c. Loss measurements shall be taken from both ends at applicable wavelengths as in subparagraphs i and ii above, and in compliance with OFSTP-7 and OFSTP-14 or EIA/TIA-568 B as applicable.
    d. OTDR measurements shall be performed for each fiber for length, transmission anomalies, and end-to-end attenuation.

   e. A written report shall be issued and delivered to the OCO for each cable, and OTDR traces and other measurements shall be included for each fiber and provided periodically as specified in the TO.

6. See Section G.8.2 for definition and how to measure.

C.2.1.7 Internet Protocol Service

The government uses Internet Protocol Service (IPS) to support a wide range of connectivity requirements that enable government users to access the Internet, government-wide intranets, and extranets. IPS will use the IP protocol suite to interconnect GFP/SRE with other government networks and the public Internet Service Provider (ISP) networks.

C.2.1.7.1 Service Description

This section provides the IPS description.

C.2.1.7.1.1 Functional Description

IPS provides transport of Internet Protocol (IP) packets.

C.2.1.7.1.2 Standards

IPS shall comply with the following standards (as updated from time to time by the applicable governing entity):

1. Internet Engineering Task Force (IETF) RFCs
2. ANSI T1
3. ITU TSS Recommendations
4. IEEE:
   a) 802.1Q
   b) 802.1P
   c) (Optional) 802.3AD
5. Metro Ethernet Forum (MEF)
6. IETF RFCs for IPv6
7. All new versions, amendments, and modifications to the above documents and standards

C.2.1.7.1.3 Connectivity

IPS shall connect:

1. Government locations, including mobile and remote users, (i.e., SDP devices such as customer routers, switches, and firewalls) to the Internet.
2. A wide range of equipment (such as notebook PCs, PDAs, etc.) via appropriate combinations of EIS services to the Internet.
3. Government locations to other networks, including those of other EIS contractors.

C.2.1.7.1.4 Technical Capabilities

The following IPS capabilities are mandatory unless marked optional:

1. The contractor shall meet applicable routing requirements in Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.
2. The contractor shall provide IPS ports at the peak data rates specified by the customer.
3. The contractor shall support appropriate access services (such as DSL, cable high speed access, PLS, or satellite) to connect customer SDPs to the contractor's IPS.
4. The contractor's network shall have:
    a) Established public peering arrangements from the contractor's network to the Internet.
    b) Private peering arrangements established from the contractor's network with redundant links to connect to its private peering partners.
    c) Support for the government-assigned and InterNIC-registered IP addresses and domain names.
    d) Primary and Secondary Domain Name Service (DNS) to provide an authoritative name server for the customer.
5. The contractor shall provide support for the Border Gateway Protocol (BGP) for EIS customers with registered Autonomous System (AS) numbers.
6. The contractor shall validate routing protocol information using authenticated protocols. BGP sessions shall be configured in accordance with, but not limited to, the NIST SP 800-54 recommendation that BGP sessions are protected with the MD5 signature option.

C.2.1.7.2 Features

The IPS feature is mandatory.

ID Number	Name of Feature	Description
1	Class of Service (CoS)	The contractor shall accommodate and optimize an agency's applications to enable the network to accurately and consistently allow for traffic prioritization and cost-efficiencies. The Classes of Service or prioritization levels may be categorized as: 1. Premium — for time-critical traffic such as voice and video 2. Enhanced — for business-critical traffic such as transactions 3. Standard — for non-critical traffic such as email.

C.2.1.7.3 Interfaces

These UNIs at the SDP for the provisioning of IPS are mandatory unless marked optional.

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type
1 (Optional)	Cable High Speed Access	25 Mbps download, 5 Mbps upload and above (DOCSIS 3.x or latest standard)	Point-to-Point Protocol, IPv4/v6
2	Ethernet Interface	1. 1 Mbps up to 1 GbE (Gigabit Ethernet) 2. 10 GbE and above (Optional) 3. Burstable	IPv4/v6 over Ethernet
3	IP over SONET Service	1. OC-3c 2. OC-12c 3. OC-48c 4. OC-192c	IP/PPP over SONET
4	Private Line Service	1. DS0 2. T1 3. T3 4. OC-3c 5. OC-12c 6. OC-48c 7. OC-192c	IPv4/v6 over PLS
5 (Optional)	DSL Service	xDSL access at 1.5 Mbps download and above, and 384 Kbps upload and above	Point-to-Point Protocol, IPv4/v6
6 (Optional)	FTTP	256 Kbps and above	Point-to-Point Protocol, IPv4/v6

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type
7 (Optional)	Wireless Access	1. 4G LTE, 5G and future evolutions 2. Satellite	Point-to-Point Protocol, IPv4/v6

C.2.1.7.4 Performance Metrics

The performance levels and AQL of KPIs for IPS are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Av(Port)	Routine	99.95%	≥ 99.95%	See Note 1
	Critical	99.995%	≥ 99.995%	
Latency (CONUS)	Routine	60 ms	≤ 60 ms	See Note 2
	Critical	50 ms	≤ 50 ms	
GOS (Data Delivery Rate)	Routine	99.9%	≥ 99.9%	See Note 3
	Critical	99.99%	≥ 99.99%	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 4
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Port availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the port is operationally available to the agency. Availability is computed by the standard formula:

$$Av(Port) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Latency is the average time for IP packets to travel across the contractor's infrastructure. The Latency metric does not apply for the DSL, Cable High Speed, Wireless, and Satellite access methods. Packet delivery and latency can be calculated using the Internet Control Message Protocol (ICMP) test, in which a series of five test packets is sent every five minutes between contractor service aggregation points (i.e., POPs). The test results are analyzed to determine

packet loss vs. successful delivery and speed of delivery. The relevant standards are RFC 1242 and RFC 2285.

3. Network packet delivery is a measure of IP packets successfully sent and received across the contractor’s infrastructure. The data delivery rate can be measured with the ICMP test (Data Delivery Rate %) = (100 - Packet Loss %).
4. See Section G.8.2 for the definitions and measurement guidelines.

C.2.1.8 Broadband Internet Service

The government uses Broadband Internet Service (BIS) to support a wide range of connectivity requirements. BIS will use the IP protocol suite to interconnect GFP/SRE with other government networks and the public Internet Service Provider (ISP) networks.

Use cases for BIS include supporting SD-WAN service as an underlay, potential direct connections to Cloud Service Providers, low cost network connectivity to Agency networks, Wi-Fi backhaul for public facing agencies customers and guests, and services for geographic areas where other network transport services are limited or non-existent.

C.2.1.8.1 Service Description

Broadband Internet Service provides high-speed Internet access that is always on. Broadband Internet Service includes several high-speed transmission technologies such as those listed in Section C.2.1.8.3.

C.2.1.8.1.1 Functional Description

BIS provides transport of Internet Protocol (IP) packets.

C.2.1.8.1.2 Standards

BIS shall comply with Federal Standards listed in Section C.1.8 as they apply to the service.

C.2.1.8.1.3 Connectivity

BIS shall connect:

1. Government locations, including mobile and remote users, (i.e., SDP devices such as customer routers, switches, and firewalls) to the Internet.
2. A wide range of equipment (such as notebook PCs, Mobile devices, etc.) via appropriate combinations of EIS services to the Internet.
3. Government locations to other networks, including those of other EIS contractors.

4. Non-Government locations, including Partners, Local Exchange Carriers (LECs), Collaborators (educational activities such as Universities).

C.2.1.8.1.4 Technical Capabilities

The following BIS capabilities are mandatory unless marked optional:

1. The contractor shall meet applicable routing requirements in Section C.1.8.8.
2. All BIS port access components shall equal or exceed the download bandwidth of the port with which it is embedded.
3. The contractor shall include appropriate embedded asymmetric or symmetric access services (such as high speed access over copper or fiber optic cable, DSL, wireless or satellite) to connect customer SDPs to the contractor's BIS as part of the service. Separately priced Access Arrangements are not required for BIS.
4. The contractor shall not impose a limit or throttle on the data downloaded or uploaded during the billing period.
5. The contractor's network shall have:
   a) Established public peering arrangements from the contractor's network to the Internet.
   b) Private peering arrangements established from the contractor's network with redundant links to connect to its private peering partners.
   c) Support for the government-assigned and InterNIC-registered IP addresses and domain names.
   d) Primary and Secondary Domain Name Service (DNS) to provide an authoritative name server for the customer.
   e) Albility to designate dynamic or fixed IP addresses for customer equipment.

C.2.1.8.2 Features

The listed BIS features are optional.

ID Number	Name of Feature	Description
1	BIS Enhanced Class of Service (CoS) (Optional)	The contractor shall accommodate and optimize an agency's applications to enable the network to accurately and consistently allow for traffic prioritization and cost-efficiencies. Some providers of BIS may not be able to provide CoS as part of the standard BIS service without additional SRE. The Classes of Service or prioritization levels may be categorized as shown

ID Number	Name of Feature	Description
		in the examples below: 1. Enhanced — for business-critical traffic such as transactions, and SD-WAN control/data plane communications
2	Static IP Address (Optional)	The contractor shall provide static IPv4/IPv6 addresses with the BIS service.

C.2.1.8.3 Interfaces

These UNIs at the SDP for the provisioning of BIS are mandatory unless marked optional.

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type
1	Cable Access	25 Mbps download, 5 Mbps upload and above (DOCSIS 3.x or latest standard)	IPv4/v6
2	Ethernet Interface	10 Mbps and above (sub-interfaces of lesser capacity shall be made available to meet customer requests where feasible)	IPv4/v6 over Ethernet
3 (Optional)	DSL Service	xDSL access from 25 Mbps and above download, and from 5 Mbps and above upload	Point-to-Point Protocol, IPv4/v6
4 (Optional)	FTTP	25 Mbps and above	IPv4/v6
5	Fixed Wireless Access	1. 4G LTE 2. 5G and future evolutions 3. 802.11x 4. Satellite (optional)	IPv4/v6

C.2.1.8.4 Performance Metrics

The performance levels (KPIs) for BIS are mandatory and are as follows:

Broadband Internet Service Performance Metrics:

- Availability (Port): Best effort

KPI	Service Level	Performance Standard (Threshold)	How Measured
Time to Restore (TTR)	Without Dispatch	24 hours	See Note 1
	With Dispatch	48 hours	

Notes:

1. See Section G.8.2 for the definitions and measurement guidelines.

C.2.2 Voice Service

The technical requirements for Voice Service (VS) are provided in Sections C.2.2.1 and C.2.2.2.

VS can be provided using various technologies. The services are organized as follows:

1. Internet Protocol Voice Service
2. Circuit Switched Voice Service

The contractor shall provide at least one of the VS technologies specified above as its mandatory VS solution. The contractor may propose to provide both forms of VS.

C.2.2.1 Internet Protocol Voice Service

Internet Protocol Voice Service (IPVS) provides voice communications service and telephony features to agencies using VoIP over a managed IP network.

C.2.2.1.1 Service Description

IPVS shall provide a network-based (hosted) and premises-based telephone service over the contractor-provided IP network. The contractor shall also provide a Managed LAN Service (see Section C.2.2.1.5) and Session Initiation Protocol (SIP) Trunking Service (see Section C.2.2.1.6).

C.2.2.1.1.1 Functional Definition

IPVS supports voice calls, whether initiated from on-net or off-net locations, to be connected to all on-net and off-net locations by direct dialing.

C.2.2.1.1.2 Standards

IPVS shall comply with the following standards (as updated from time to time by the applicable governing entity):

1. ITU-T G.711
2. (Optional) ITU-T G.723.x, G.726, G.728, or G.729.x
3. ITU-T H.323, H.350
4. Real-Time Transport Protocol (RTP) IETF RFC 3550
5. Session Initiation Protocol (SIP) IETF RFC 3261

C.2.2.1.1.3 Connectivity

IPVS shall connect to and interoperate with wireline and wireless networks, other EIS contractor voice networks, and satellite-based voice networks, in both domestic and non-domestic locations, using interconnects to the PSTN.

C.2.2.1.1.4 Technical Capabilities

The IPVS shall include unlimited on-net to on-net and on-net to CONUS off-net calling. The IPVS shall support off-net calling to CONUS, OCONUS, and Non-Domestic locations. The contractor shall provide capabilities that enable IPVS users to establish and receive telephone calls between both on-net locations and the PSTN.

The contractor shall provide a remote access capability that, once enabled, provides users with the ability to use any landline or cell phone to make or receive phone calls as if they were making or receiving calls with VoIP phones.

The following capabilities are mandatory unless marked optional:

1. Real time transport of voice, facsimile, and TTY communications
2. Real time delivery of Automatic Number Identification (ANI) information (when provided from the originating party)
3. Interoperate with public network dial plans (e.g., North American Numbering Plan and ITU-E.164)
4. Interoperate with private network dial plans and support direct dialing
5. (Optional) Interoperate with non-commercial, agency-specific 700 numbers
6. Provide access to public directory and operator assistance services
7. Provide unique directory numbers for all on-net government locations, including support for existing government numbers.
8. Provide the capability to initiate automatic callback
9. Support 3-way calling

The contractor shall provide gateways for interoperability between the contractor's IP-based network and the PSTN, or with agency UNIs. The specific gateway will depend upon the ordering agencies UNI requirements. The gateways and functionality are described below:

1. Subscriber Gateway – The contractor shall provide interoperability for non-IP telephone devices. The contractor shall provide non-proprietary telephony station UNIs including (a) analog station and (b) ISDN BRI station interfaces.
2. PSTN Gateway – The contractor shall provide transparent access to and interwork with the domestic and non-domestic PSTNs.

The contractor shall provide the capability to support station mobility. Station mobility enables IP subscribers to dynamically move IP phones within the agency's enterprise wide network and access IP services.

The contractor's IPVS shall have the capability to traverse and successfully interoperate with agency firewalls and security layers. The contractor shall verify with the agency that the agency firewall is compatible with the contractor's service.

The contractor shall ensure that security practices and safeguards are provided to minimize susceptibility to security issues and prevent unauthorized access. This includes SIP-specific gateway security for SIP firewalls, where applicable. The contractor shall ensure that security practices and policies are regularly updated and audited. The general areas of security to be addressed are:

1. Denial of service – The contractor shall provide safeguards to prevent hackers, worms, or viruses from denying legitimate users from accessing IPVS.
2. Intrusion – The contractor shall provide safeguards to mitigate attempts to illegitimately use IPVS.
3. Invasion of Privacy – The contractor shall ensure that IPVS is private and that unauthorized third parties cannot eavesdrop or intercept IPVS communication numbers, IP addresses or URLs.

The contractor shall fully comply with emergency service requirements, including 911 and E911 services, and identify the location of originating stations and route them to the appropriate Public Safety Answering Point (PSAP).

The contractor's IPVS shall comply with the Federal Communications Commission (FCC) Local Number Portability (LNP) requirements.

C.2.2.1.2 Features

The following IPVS features are mandatory unless marked optional.

ID Number	Name of Feature	Description
1	Voice Mail Box	The contractor shall offer voice mail capability that includes voice messaging transmission, reception, and storage 24x7 except for periodic scheduled maintenance. The contractor-provided voice mailbox shall meet the following minimum requirements: 1. At least sixty minutes of storage time (or 30 messages) 2. Ability to remotely access voice mail services 3. Secure access to voice mail via a password or PIN 4. Automatic notification when a message is received 5. Minimum message length of two minutes 6. Capability to record custom voice mail greetings This capability can be administered on a station basis according to the ordering agency's needs. The contractor shall send an email with a WAVE (.wav) file attachment of each voicemail message received by users of this feature to the email address that the user designates. The contractor shall provide users the capability to add other notification devices / email addresses or to update email information and email preferences when receiving and forwarding messages through a secure user web portal.
2	Auto Attendant	Auto Attendant allows callers to be automatically transferred to an extension without the intervention of an operator. The contractor shall provide capabilities allowing callers to dial a single number for high volume call areas and to select from up to nine (9) options to be directed to various attendant positions, external phone numbers, mailboxes or to dial by name or extension at a minimum.
3	Augmented 911/E911 Service	The contractor shall appropriately populate a 911 Private Switch/Automatic Location Identification (PS/ALI) database with the government's profile which shall include all the users' telephone numbers, station locations, building location, building address, building floor, and room number during service implementation.The contractor shall provide secure remote access to the government via a client or a web browser to allow the government to maintain the government's profile on an ongoing basis (e.g., to account for moves, adds, deletions, or other changes). The contractor shall ensure these government profile updates are reflected in the PS/ALI database.

The following standard features shall be included in the basic service:

1. Caller ID
2. Conference Calling

3. Do Not Disturb
4. Call Forward – All
5. Call Park
6. Hotline
7. Call Forward – Busy
8. Call Pickup
9. Hunt Groups
10. Call Forward – Don't Answer
11. Class of Service Restriction
12. Multi-Line Appearance
13. Call Hold
14. Distinctive Ringing
15. Directory Assistance
16. Call Transfer
17. Call Waiting
18. Speed Dial
19. Call Number Suppression
20. Specific Call Rejection
21. Last Number Dialed
22. IP Telephony Manager (Administrator)
23. IP Telephony Manager (Subscriber)

C.2.2.1.3 Interfaces

The UNIs at the SDP are mandatory unless marked optional.

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	Router or LAN Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100 Mbps	SIP (IETF RFC 3261), H.323, MGCP, or SCCP

C.2.2.1.4 Performance Metrics

The performance levels and AQL of KPIs for IPVS are mandatory unless marked optional.

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Latency	Routine	200 ms	≤ 200 ms	See Note 1
Grade of Service (Packet Loss)	Routine	0.4%	≤ 0.4%	See Note 2
Availability	Routine	99.6%	≥ 99.6%	See Note 3
	Critical	99.9%	≥ 99.9%	
Jitter	Routine	10 ms	≤ 10 ms	See Note 4
Voice Quality	Routine	Mean Opinion Score (MOS) of 4.0	MOS ≥ 4.0	See Note 5
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 6
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Latency is the average round trip time for a packet to travel from source SDP to destination SDP. This applies to CONUS.
2. Grade of Service (Packet Loss) is defined as the percentages of packets that are sent by the source SDP but never arrive at the destination SDP (the percentage of packets that are dropped).
3. Availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the IPVS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

4. Jitter is the average variation or difference in the delay between received packets of an IP packet data stream from SDP to SDP. Relevant standard: IETF RFC 1889. This applies to CONUS.
5. As defined in ITU-T specification P.800 series.
6. See Section G.8.2 for definition and how to measure.

C.2.2.1.5 Managed LAN Service

The contractor shall provide a Managed LAN Service. The contractor shall provide and manage all LAN networking hardware components (e.g. Layer 2 switching devices, routers, switches, call servers, etc.) to extend the IPVS from the site demarcation point to the terminating user device (e.g., handset), including the management of the router that terminates the IPVS access arrangement. Equipment provided by the contractor shall support Power over Ethernet (PoE) in order to supply necessary power to IP phone sets or other PoE devices. IPVS service is a pre-requisite for Managed LAN Service.

The contractor shall provide, manage, maintain and repair or replace all equipment necessary to provide the Managed LAN Service, except for those portions of the service for which the government is responsible (e.g., power, facilities, rack space, cabling/wiring).

The contractor shall provide the technical capabilities of the Managed LAN service as specified below:

1. The contractor shall provide all hardware and licensing necessary to extend the IPVS site demarcation point to the terminating device (e.g., the handset), for both hosted and premises-based solutions. In the case of an on-premises solution this includes any hardware or licensing necessary to support on-premises call processing (e.g., call manager, IP PBX, etc.).
2. The contractor’s hardware/software solution shall interoperate with the ordering agency’s provided VoIP-ready cabling infrastructure, including category 5, 5E, 6, 6A and single mode and multimode fiber at a minimum. The contractor shall identify any cabling limitations with regard to either form of VoIP solution in its proposal.
3. The contractor shall be responsible for the ongoing maintenance and upgrades of the contractor-owned equipment used to provide the Managed LAN Service. If the contractor replaces, makes any changes to the contractor’s equipment or device software, or reprograms user devices in order to meet the required service performance level, the government will not incur any additional cost.
4. The contractor shall propose installation time intervals for additional user devices at sites already using a Managed LAN Service.
5. The Managed LAN Service shall not include any wireless devices or components on the LAN (i.e., wired solution only) unless requested and approved by the OCO.
6. The Managed LAN Service shall not support other services (i.e., data, video, etc.) unless requested and approved by the OCO.
7. The contractor shall ensure that only authorized devices (as determined by the ordering agency) are able to operate on the Managed LAN Service.
8. The contractor shall monitor, manage and restore the Managed LAN Service on a 24x7 basis.

9. The contractor shall specify the LAN management activities provided as part of the Managed LAN Service as well as identify those activities which are considered customer responsibilities in the following areas:
    a) Configuration management
    b) Moves, Adds, Changes, Disconnects (MACDs)
    c) Service/Alarm monitoring and fault management
    d) Ticket creation
    e) Proactive notification
    f) Trouble isolation and resolution
10. The contractor shall provide proactive notification of major and minor alarms to the Managed LAN Service via e-mail to the Points of Contact (POCs) identified by the ordering agency. Alarm notifications shall be sent to all identified POCs within 15 minutes of alarm detection by the contractor.
11. The contractor shall define the escalation path for trouble tickets for both network and hardware issues. This escalation path shall be identified by level of severity and shall include personnel for each level of escalation as well as guidelines and timing for the next step in escalation.

C.2.2.1.6 Session Initiation Protocol Trunk Service

Session Initiation Protocol (SIP) Trunk Service provides a SIP-based IP Trunk service that interoperates with any Private Branch Exchange (PBX) systems that support SIP-based IP Trunk interfaces.

SIP Trunk Service provides a direct IP connection between a SIP-enabled PBX system on an agency's premises and the contractor's SIP-compliant IPVS network. SIP trunking shall be fully integrated with IPVS to support calling to on-net and off-net locations. The network and its management will be provided by the underlying network service.

C.2.2.1.6.1 Technical Capabilities

The contractor shall provide capabilities that enable SIP users to successfully establish and receive telephone calls between both on-net locations and the PSTN.

C.2.2.1.6.2 Features

The following SIP Trunk Service features are mandatory unless marked optional.

1. Automatic call routing
2. Bandwidth QoS management
3. Trunk bursting
4. Telephone number blocks (DID)

C.2.2.2 Circuit Switched Voice Service

The government has a large community of circuit-switched voice users throughout the US public sector and also conducts a considerable amount of business with US citizens, private sector firms, and foreign entities using circuit-switched voice.

C.2.2.2.1 Service Description

C.2.2.2.1.1 Functional Definition

Circuit Switched Voice Service (CSVS) supports voice calls, whether initiated from on-net or off-net locations, to be connected to all on-net and off-net locations by direct dialing throughout the US. The government's requirement for CSVS is functional.

C.2.2.2.1.2 Standards

The contractor shall comply with voice service industry standards.

C.2.2.2.1.3 Connectivity

CSVS shall connect to and interoperate with:

1. Government-specified terminations (such as single-line telephones, Secure Terminal Equipment, multi-line key telephone systems, conference-room audio equipment, PBX, Centrex, T1 MUX, modem, FAX, and video teleconferencing systems).
2. PSTN, including both wireline and wireless networks, in domestic and non-domestic locations.
3. The voice service networks of all other EIS contractors.
4. Satellite phones and terminals.

C.2.2.2.1.4 Technical Capabilities

The following VS capabilities are mandatory unless marked optional:

1. Numbering plan:
    a) Unique directory number for all on-net government locations, including support for existing government numbers.
    b) PSTN (including both wireline and wireless networks) numbers and any future changes to PSTN numbers.
    c) (Optional) Non-commercial agency-specific private 700 numbers:
        i. Originating and terminating on-net calls. Incoming off-net calls from the PSTN shall be blocked unless an agency-specific request for the service gateway has been received and implemented.

   d) Transparency and interconnectivity between the contractor’s network and other networks (see Section C.2.2.2.1.3).

2. Network intercept. Network intercept to a recorded announcement shall be provided as an inherent network capability when a call cannot be completed. At a minimum, such announcements shall be provided for the following conditions:
   a) Number disconnected (a disconnected number shall not be reassigned for at least 90 days if the contractor controls number assignment)
   b) Time-out during dialing
   c) Network congestion
   d) Denial of access to off-net and non-US calls
   e) Denial of access to features
3. (Optional) User-to-user signaling via ISDN D-Channel. The contractor shall support user-to-user signaling in accordance with ITU-TSS Q.931 standards, via the ISDN D-channel during a call.
4. Voice quality at least equal to 64 kbps PCM (standard: ITU G.711).
5. The contractor shall fully comply with emergency service requirements, including 911 and E911 services, and identify the locations of originating stations and route them to the appropriate Public Safety Answering Point (PSAP).

C.2.2.2.2 Features

The following CSVS features are mandatory unless marked optional:

ID Number	Name of Feature	Description
1	Agency-Recorded Message Announcements	1. Authorized government personnel shall be able to record message announcements within the network after authentication of user-ID and password/token. 2. The recording shall be assigned an on-net number and shall be accessible from on-net and off-net stations. 3. The contractor shall provide the capability of a three-minute message announcement length. 4. The length of each message provided by the government will be determined on a case-by-case basis and will continue to three minutes in length (or longer if the contractor capability exists and is provided at no additional cost to the government).

ID Number	Name of Feature	Description
		5. A call to the announcement must be answered within five rings and barge-in access to the announcement shall be permitted. 6. The contractor shall provide a system-wide capability for storing a minimum of 500 recorded messages. This feature shall enable a minimum of 250 callers concurrently to access an announcement.
2 (optional)	Authorization Codes/ Calling Cards	The contractor shall provide authorization codes that support the following functions: 1. Caller identification and class-of-service (CoS) for users to include call screening (see User's Call Screening feature) and service performance levels (see Performance Metrics for routine and critical users). At a minimum, 128 classes of service shall be available to each user, station, or trunk. 2. Same authorization code for originating on-net, off-net, and audio conference calls. 3. Use authorization code if originating station identification cannot be made by other means for billing and CoS purposes. 4. Use authorization code when override capabilities are desired. 5. The CoS derived from an authorization code shall take precedence over that derived from any other means. 6. When an authorization code is used for the service, it shall be verified without involving an operator before a call is connected. 7. The contractor shall support the following capabilities as specified by the government: a. Actual requirements for calling party identification (e.g., ANI suppression). b. CoS assignment. c. Types of calling cards: 1. Post-paid calling cards. (a) Charges accumulate as the card is used, and billing is based upon monthly charges.

ID Number	Name of Feature	Description
		2. Pre-paid calling cards. (a) Fixed dollar amount of $50.00 (b) Rechargeable dollar amount where amount can be renewed or increased when the initial amount balance is low or depleted d. Expiration date for pre-paid calling cards. e. Use for audio conferencing service (ACS) only. f. Agency-specific logo and no printing of GSA logo on the card. g. Suppression of call detail records (CDRs). h. Immediate cancellation of the card if reported stolen or lost by a user without incurring further charges on the card. The format of the authorization code shall be determined by the contractor and shall support/provide the following capabilities: 1. Credit card-sized authorization code card(s), also called Calling Cards, unless otherwise directed by the government. 2. Durable plastic composition and imprinted with authorization code, user's name, and organization. 3. User instructions shall be issued, as directed by the government, at no additional cost. 4. Safeguards as follows: a. Potential fraud and theft regarding issuance, distribution, and activation of authorization codes. b. Delivery of Personal Identification Numbers (PINs) independent from delivery of the calling cards. c. Exclusion of the last 4 digits of authorization codes (i.e., PINs) in billing records. 5. If sufficient space is available, inclusion of the Federal Relay Service's "TDD/800-877-8339" number on the back of the calling card. 6. Contractor-defined dialing sequence that alerts the network when an authorization code is about to be entered so that processing of calls not requiring this feature are not delayed.

ID Number	Name of Feature	Description
		7. Temporary override of a CoS restriction assigned to a caller's station. This will allow an individual user to place a call at a higher network CoS for the duration of the call by entering a valid authorization code. This capability shall have the following functionalities. a. Absence of excessive delays caused by waiting for all digits to be dialed before recognizing the call as one that involves an override. b. Inclusion of all CDR relevant data charged to the authorization code rather than to the originating station. 8. Allowance of authorized users to gain access, after validation of authorization codes, to on-net voice service and features from off-net locations by dialing certain contractor-provided toll free and message unit-free (to the callers) commercial directory numbers. This capability shall have following functions. a. Numbers may be a local number, a Foreign Exchange number, an NANP number, or some other service type, e.g., toll free service, for which toll free and message unit-free service has been arranged for pre-designated regions. b. Toll free and message unit-free commercial directory numbers shall be printed on the back of the calling card. c. Region boundaries shall be defined by the contractor. d. Users shall be able to select, by service order, the regions of the country from which access is to be allowed and the service type that provides the most economical service for a given application. 9. A multiple call feature that shall allow the user to dial a code (e.g., the "pound" key [#]) after a call in order to make multiple calls without re-dialing the access and card number. 10. Direct operator access to provide assistance with dialing or for providing information. 11. An error correction feature that enables cardholders to correct a dialing mistake by pressing a key, e.g., the "star" key (*) and re-enter the correct number.

ID Number	Name of Feature	Description
		12. Speed dialing that allows cardholders to use abbreviated dial codes for frequently dialed numbers. 13. Availability of all administrative tools or management reports made available by the contractor with equivalent commercial calling card offerings.
3	Caller Identification (ID)	The contractor shall provide the calling number to the terminating stations for each incoming call.
4 4.2. (optional)	Call Screening for users	Call screening consists of a set of features that determine a call's eligibility to be completed as dialed based upon CoS information associated with the user, the station, or the trunk group. The following call screening features shall be supported: 1. Class of Service (CoS) and Restrictions. The contractor shall provide a minimum of 128 classes of service for each user, station, or trunk. CoS shall be determined from the ANI, authorization code, traveling classmark, or trunk group. The CoS derived from an authorization code shall take precedence over that derived from other means. Classes of service shall identify but not be limited to access and feature restrictions as follows: a. Access restrictions shall include but not be limited to access to toll free and 900 calls, access to off-net calling, access to other government networks, access to non-US calling, and access to other than specified NPA/NXXs. b. Feature restrictions shall allow or restrict access to network features by users or groups of users. 2. Code Block. This feature shall screen and prevent ineligible users, stations, and trunks with certain CoS access restrictions from calling specified area codes, exchange codes, and countries. Blocked calls shall be intercepted to appropriate network recorded announcements.
5 (optional)	Customized Network Announcement Intercept Scripts	The contractor shall implement customized network intercept announcement scripts as requested by the government. The contractor shall record the customized network announcements after obtaining government approval of scripts.

ID Number	Name of Feature	Description
6 (optional)	Internal Agency Accounting Code	For calls involving a calling card or originating station with a special CoS, the following capabilities shall be provided: 1. Entry of additional (up to a maximum of eight) digits to identify internal agency accounting codes for the call, i.e., these accounting codes will be transferred to the CDR with no further processing. 2. CDRs shall reflect all relevant data on the call to include internal agency accounting code digits. Calls shall be charged to the authorization code rather than to the originating station.
7	Directory Assistance	A user shall be able to call off-net directory assistance by dialing NPA-555-1212 or any other off-net directory assistance number. NPA also includes service access codes (e.g., 800) for this feature.
8	Suppression of Calling Number Delivery	Based on the CoS of the originating station or calling card, the contractor shall inhibit the delivery of the calling number, i.e., ANI, by setting the Privacy Indicator at the originating end and honoring it at the terminating end. In addition, it shall be possible to block calling number delivery on a call by call basis by dialing a contractor-provided code.
9	Voice Mail Box	The contractor shall offer voice mail capability that includes voice messaging transmission, reception, and storage for 24x7 except for periodic scheduled maintenance. The contractor provided voice mailbox shall meet the following minimum requirements: 1. At least sixty minutes of storage time (or 30 messages) 2. Ability to remotely access voice mail services 3. Secure access to voice mail via a password or PIN 4. Automatic notification when a message is received 5. Minimum message length of two minutes 6. Capability to record custom voice mail greetings This capability can be administered on a station basis according to the ordering agency’s needs.
10 (optional)	Basic Subscriber Line: Multi Appearance Directory Number	A Multiple Appearance Directory Number is a telephone number that appears on two or more telephones.

ID Number	Name of Feature	Description
11 (optional)	ISDN PRI: Backup of Shared-D Channel	Backup of a single D channel that is controlling multiple PRIs.
12 (optional)	ISDN BRI: Multi Appearance Directory Number	A Multiple Appearance Directory Number is a telephone number that appears on two or more ISDN telephones.
13 (optional)	MLPP	DOD requires the CSVS to have Multilevel Precedence and Preemption (MLPP) capability as defined in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C and DOD Instruction 8100.3, Department of Defense Voice Networks, to specified users and on trunks connecting to the Defense Switched Network (DSN).

C.2.2.2.3 Interfaces

The UNIs at the SDP are mandatory unless marked optional:

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	Analog Line: Two-Wire (Basic Subscriber Line) (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Line-Loop Signaling
2	Analog Line: Four-Wire (Basic Subscriber Line) (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Line-Loop Signaling
3	Analog Trunk: Two-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk-Loop Signaling (loop and ground start)

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
4	Analog Trunk: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk–Wink Start Signaling
5	Analog Trunk: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk-E&M Signaling
6	Digital Trunk: T1 (Std: Telcordia SR-TSV-002275 and ANSI T1.102/107/403)	Up to 1.536 Mbps	T1 Robbed-Bit Signaling
7	Digital Trunk: ISDN PRI (23B+D and 24B+0D)T Reference Point (Std: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931
8	Digital: T3 Channelized (Std: Telcordia GR-499-CORE)	Up to 43.008 Mbps	SS7, T1 Robbed-Bit Signaling
9 (Non-US)	Digital Trunk: E1 Channelized (Std: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling
10 (Optional)	Optical: SONET OC-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	SS7
11 (Optional)	Electrical: SONET STS-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	SS7

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
12 (Non-US)	Digital: E3 Channelized (Std: ITU-TSS G.702)	Up to 30.72 Mbps	SS7, E1 Signaling
13	Digital Line: ISDN BRI (2B+D) S and T Reference Point (Std: ANSI T1.607 and 610)	Up to 128 kbps (2x64 kbps)	ITU-TSS Q.931
14	Router or LAN Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100 Mbps	SIP (IETF RFC 3261), H.323, MGCP, or SCCP

C.2.2.2.4 Performance Metrics

The performance levels and AQL of KPIs for CSVS are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability (POP-to-POP)	Routine	99.95%	≥ 99.95%	See Note 1
Availability (SDP-to-SDP)	Routine	99.5%	≥ 99.5%	
	Critical	99.95%	≥ 99.95%	
Time to Restore	With Dispatch	8 hours	≤ 8 hours	See Note 2
	Without Dispatch	4 hours	≤ 4 hours	
	Routine	0.07 (SDP-to-SDP)	≤ 0.07	See Note 3
		0.01 (POP-to-POP)	≤ 0.01	

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Grade of Service (Call Blockage)	Critical	0.01 (SDP-to-SDP & POP-to-POP)	< 0.01	

Notes:

1. CSVS availability is calculated as a percentage of the total reporting interval time that the voice service is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

[Note that this KPI is waived for calls made with calling card.]

2. Refer to Section G.8.2 for definition and how to measure.
3. Grade of Service (Call Blockage) is the proportion of calls that cannot be completed during the busy hour because of limits in the call handling capacity of one or more network elements. For example, 0.01 indicates that 1 percent of the calls are not being completed (1 out of 100 calls).

C.2.2.3 Toll Free Service

C.2.2.3.1 Service Description

Agencies can use inbound Toll Free Service (TFS) as a convenient means of accessibility for different callers including citizens, non-citizens, and agency personnel. TFS includes a set of advanced service features and related voice applications to meet agency needs for delivering services to their callers.

C.2.2.3.1.1 Functional Definition

Toll Free Service provides basic inbound toll free calling and offers advanced feature and call routing capabilities. TFS includes intelligent call routing and network-based Interactive Voice Response (IVR) capabilities to enable agencies to effectively manage inbound calls.

C.2.2.3.1.2 Standards

Toll Free Service shall comply with the following standards:

1. ITU-T standard E.164 as interpreted by the Industry Number Committee of the Alliance for Telecommunications Industry Solutions (ATIS). The contractor shall support the following numbering schemes:
    a) For domestic (CONUS and OCONUS) service, numbering shall be consistent with 800, 888, 877, 866, and other toll-free non-geographic codes available from the SMS/800 database managed by Telcordia.
    b) For non-domestic service, numbering shall be consistent with requirements or practices in the country in which the call originates.
2. ITU-T P.800 series of standards for telephone transmission quality.
3. The contractor shall comply with new versions, amendments, and modifications made to the above listed documents and standards.

C.2.2.3.1.3 Connectivity

Toll Free Service shall connect to and interoperate with the PSTN including both wireline and wireless. TFS uses underlying Voice Service for connectivity as delineated in Section C.2.2.2.1. TFS shall be provided for both dedicated and switched terminating access arrangements.

C.2.2.3.1.4 Technical Capabilities

The following TFS capabilities are mandatory unless marked optional.

1. The contractor shall act as the responsible organization or “Resp Org” for assignment and maintenance of toll-free numbers if requested by the ordering agency.
2. The contractor shall support toll-free number portability.
3. The contractor shall accommodate any presently assigned agency toll-free numbers.
4. When requested by an ordering agency, the contractor shall offer Universal International Toll-Free Number service (also known as Universal International Free Phone Number - UIFN). This shall enable the agency to request a single, unique toll-free number that is the same throughout the world (where available commercially from participating countries).
5. The contractor shall provide the capability for a single toll-free number to terminate at multiple locations (SDPs) and multiple toll-free numbers to terminate at a single location (SDP).

6. As a default measure, the contractor shall provide a busy signal or recorded announcement for all calls that encounter network congestion and/or terminating egress congestion, as determined by the ordering agency.
7. The contractor shall provide a network intercept to record announcements as an inherent network capability when a call cannot be completed. At a minimum, such generic announcements shall be provided for the following conditions:
   a) Time out during dialing
   b) Denial of access to features and other related conditions
   c) Denial of access to non-domestic or restricted calls
8. The contractor shall provide the capability for customized network intercept recorded announcements. The contractor shall provide options for the custom announcement to be a) recorded by the contractor or b) recorded remotely by the ordering agency.
9. The contractor shall, at a minimum, provide the capability to have all announcements recorded in English and Spanish languages. Other languages shall be optional.
10. The contractor shall provide a referral message to callers of a disconnected toll-free number. Upon a submission of a TFS disconnect order; the agency shall have the option for a referral telephone number to be provided in an announcement message to callers of the disconnected toll-free number.
11. The contractor shall provide Dialed Number Identification Service (DNIS). DNIS will enable multiple toll-free numbers to be routed and uniquely identified on a shared trunk group. The contractor shall transmit DNIS digits, upon agency request, prior to the delivery of a TFS call to uniquely identify the dialed toll-free number. The DNIS digit length shall range from 3 to a maximum of 10 digits.
12. The contractor shall identify and provide the calling parties Automatic Number Identification (ANI) to assist agencies with identifying malicious or emergency calls.

C.2.2.3.2 Features

The following Toll Free Service features are mandatory unless marked optional.

These features shall be capable of being used independently of each other or in any combination except where noted in the contract. The combination of features associated with routing functions unique with each toll-free number shall constitute a “Call Routing Plan.” Call Routing Plans shall be subject to control by the ordering agency via the Routing Control feature described in this section.

ID Number	Name of Feature	Description
1	Agency-based routing database (also known as Host Connect)	The contractor shall provide the ability to route TFS calls or provide information based upon a query(s) of information provided by a database located at the ordering agency premises. The query(s) could be to single, redundant, or multiple databases, depending upon agency specifications and the complexity of the application. The contractor shall implement and provide the appropriate interface and connectivity for the contractor's IVR application to successfully query and access an ordering agency's database(s). The IVR caller shall have the capability to retrieve, review, and modify information located on the agency database based upon ordering agency needs. The agency database(s) can be a (1) mainframe or (2) server-based relational database. If the database does not respond to the network query within 250 milliseconds, an agency-defined default routing plan shall be used.
2	Alternate Routing (also known as "Cascade" routing)	The contractor shall allow TFS calls to be re-routed on a pre-determined plan based upon availability of trunks (busy) at the terminating location, a maximum number of calls allowed in progress, or a pre-defined ring-no-answer condition. If none of the alternate terminations are able to receive the call, then the call shall be terminated to (1) a predefined announcement, or (2) a busy signal, at the ordering agency's option.
3	ANI	Automatic Number Identification (ANI). The contractor shall allow transmission of the TFS caller's real time ANI information (full 10 digit number or non-domestic equivalent) to the ordering agency.
4	ANI Based Routing	The contractor shall enable TFS calls to be routed based upon the originating ANI of the caller. Default routing defined by the ordering agency shall be used if ANI is not available.
5	Announced Connect	The contractor shall provide a customized message to the called party, before the TFS caller is connected, and provide the called party with information about the caller (e.g. ANI, account number etc.). This feature is commonly referred to as a "whisper."
6	Announcements	The contractor shall provide TFS network-based announcements with both generic and customized recordings. For customized recordings, the agency shall have the option to record the custom announcement script or have the contractor record the script. At a minimum, the announcements should be available in (1) English, (2) Spanish, and (3) (optional) other languages. At

ID Number	Name of Feature	Description
		an agency's request, the contractor shall provide the option for a forced disconnect after the announcement recording is played.
7	Menu Routing	The contractor shall allow TFS callers to be provided with informational messages and be routed according to information entered via DTMF signal or via speech. The contractor's call prompter shall provide, at a minimum, the following capabilities: 1. Select pre-recorded announcement messages with the capability for announcements. Such announcements shall always be played from the beginning for each caller and provide the capability to be recorded in English and other languages after obtaining ordering agency script approval. 2. The contractor shall provide the ability to transfer out ("menu routing") during an announcement to an agency-specified predefined termination with an option to return back an announcement/menu without needing to redial. 3. The contractor shall support multi-tiered prompting (menus) such that another series of options can be provided to the caller after making the initial menu selection, and provide routing to an agency designed default location if no caller input is entered. 4. The contractor shall provide the ability for the caller to leave information via DTMF signal or speech (e.g., names, addresses, account information, phone numbers) for transcription or reporting purposes. For speech transcription, the contractor shall provide a) transmission of the recorded voice files and DTMF data for each transaction to the agency and b) a report of caller responses that transcribes the caller provided information for the ordering agency based upon an ordering agency's needs and transmits it to the agency. The contractor shall provide transcription reports from English and Spanish speaking callers. 5. The contractor shall provide a capability that allows callers to hear and verify their names and addresses in an agency-provided name and address database after the caller has entered his or her telephone number via DTMF, or based on the caller's ANI. 6. The contractor shall provide a means for the ordering agency to retrieve caller-entered DTMF or speech messages. 7. Upon agency request, the contractor shall offer the option for a forced disconnect after an announcement recording is played.
8	Call Redirection	The contractor shall enable TFS calls to be transferred by the contractor's network, no matter which platform the call is being

ID Number	Name of Feature	Description
		re-directed from, from the called party/agent to another toll-free number or any PSTN number by using, at the agency's discretion, any one of the three following modes of network level call transfer: 1. Blind transfer (unsupervised) 2. Verification by the agent and then transfer (supervised) 3. Three-way conference and then transfer The contractor shall ensure that there is no double billing for toll free calls that have been transferred using call redirection. This includes calls redirected within the contractor's network from one operating platform to another operating platform. In addition, the contractor shall offer the ability to put the caller on hold and provide abbreviated dialing codes. The contractor shall state the amount of abbreviated-dial codes available for use with this feature. The contractor shall provide two options for music on hold during the call redirection – either contractor provided or from an agency-provided source.
9	Computer Telephony Integration (CTI)	The contractor shall provide CTI messaging capability that enables transfer of caller information and agency-specified data between the TFS contractor and agency-specified systems simultaneously with the associated inbound toll-free call. This feature can be used to support a diverse set of applications such as screen pop/splash, intelligent call routing, enhanced reporting, third party call control and multi-channel call blending solutions.
10	Custom Call Records	This feature shall be used in conjunction with the TFS Interactive Voice Response and Call Prompter features. The contractor shall provide individual call detail data records which include, at a minimum, the following data: 1. Date and time of TFS call 2. Call duration 3. Specific details regarding the call attempt (e.g., menu options selected in an IVR or Call Prompter application) 4. Call entered digits 5. Call disposition (busy, complete, no answer, blocked) 6. Caller information (ANI - if available or DNIS) 7. Toll-free number dialed 8. Flexible custom fields according to agency needs

ID Number	Name of Feature	Description
		The contractor shall provide a detailed description of each call detail record field including definitions of the data elements prior to activation of the feature. The format of the call record data shall be such that it can be easily imported into agency databases or applications. The call records and a summary report should be available electronically on a daily, weekly or monthly basis as requested by the ordering agency.
11	Day of Week Routing	This contractor shall enable TFS calls to be routed to different terminations or applications based upon the day of week.
12	Day of Year Routing (Holiday Routing)	The contractor shall enable TFS calls to be routed to different terminations or applications based upon the day of the year. A minimum of ten dates should be eligible during a twelve month period for day of year routing.
13	In Route Announcements	This feature shall allow TFS callers to hear an announcement during call setup without affecting the final termination/route of the call. At a minimum, announcements shall be available in either (1) English or (2) Spanish and (3) (optional) other languages.
14	Interactive Voice Response (IVR)	The contractor shall provide an automated application that provides TFS callers with information based upon input from either (a) DTMF key entries or (b).natural speech recognition. The contractor shall provide the minimum required capabilities listed below: 1. Select pre-recorded announcement messages with the capability for announcements and offer the ability for a caller to opt out during an announcement to a predefined termination and an option to return back an announcement without needing to redial. Such announcements shall always be played from the beginning for each caller and provide the capability to be recorded in English and other languages. 2. Leave caller information via DTMF signal or speech (e.g., name, address, account information, etc.). For transcription of caller information, the contractor shall provide a) transmission of the recorded voice files and DTMF data to the agency and b) a report of caller responses that transcribes the caller provided information for the ordering agency based upon the ordering agency's needs and transmits it to the agency. The contractor shall provide transcription reports from English and Spanish speaking callers.

ID Number	Name of Feature	Description
		3. The contractor shall provide a means for the ordering agency to retrieve caller-entered DTMF or speech messages. 4. The contractor shall query a database that delivers agency-provided information to the caller. The database may be located at the ordering agency or, at the ordering agency's discretion, located at a contractor location and updated by the ordering agency. Provide a default routing or message (agency option) if the database is unavailable. 5. The contractor shall provide a capability to allow callers to hear and verify their names and addresses in an agency-provided name, address, and zip code database after the caller has entered his or her telephone number via DTMF, or based on the caller's ANI (Text to Speech). 6. The contractor shall support speech recognition as a valid caller input. The contractor shall support at a minimum, all spoken numeric digits as well as "yes" and "no." English and Spanish language callers shall be supported. The contractor shall be able to accept and process, at a minimum, 95% of the above speech responses. Speech responses which are not accepted shall be routed to default location designated by the ordering agency. 7. The contractor shall provide the capability to perform surveys (via DTMF or speech) to IVR callers. The surveys can be provided to all or a random percentage of callers according to agency needs. Survey results shall be provided electronically to the ordering agency. 8. (Optional) The contractor shall provide a facsimile or technical equivalent "fax back" capability (Fax or equivalent) that shall permit callers to retrieve agency-specific documents or forms. The contractor shall fax back the request documents within one hour of the initial call and retry a minimum of 13 attempts over a six hour interval in order to complete the request. Fax or technical equivalent transmittal shall include an option for a cover sheet (standard or customized). 9. At the agency's option, the caller's IVR selection(s) information shall be transferred to the agency. 10. The contractor's IVR capacity must be configured such that the application answers a call within 3 ring cycles for 99 % of the offered call volume (measured on an hourly basis) during the busy hour.

ID Number	Name of Feature	Description
		11. The contractor shall provide features equivalent to the above shall be available to individuals who are hearing impaired or have speech disabilities via electronic means in Baudot and ASCII/TTY code formats. These electronic form lines need not be voice feature enabled. 12 The contractor shall provide summary reporting that at a minimum provides information on the caller, average call duration, caller opt out (transfer), and disposition of the calls within the IVR application on a daily, weekly, and monthly basis.
15	Make Busy Arrangement	The contractor shall permit the agency to deactivate one or more TFS dedicated access trunks within a trunk group, Upon deactivation, the trunk(s) shall appear in a busy state. The capability to activate and deactivate the status of the trunks shall be controlled either via software available to the ordering agency or at the agency's option by notifying the contractor. At a minimum, the request shall be executed by the contractor within one hour of request.
16	Network Call Distributor	The contractor shall provide advanced, intelligent call routing capabilities based upon real time status of each contact center's operating conditions, agent skills, and/or agency-specified business rules. The contractor shall poll all of the ordering agency's PBX/ACD's regular intervals for real-time ACD operating status information to update a call routing processor which shall use call routing logic/algorithms that have been predefined by the agency, to determine the best location or resource to deliver the inbound call. The call routing processor containing the call routing logic/algorithms shall be able to use, in the ordering agency's defined combinations, all real-time operating status information collected from the agency's PBX/ACD's. The ACD-provided information shall be polled and shall include at a minimum: 1. Number of incoming trunks 2. Number of incoming trunks available to receive a call 3. Number of calls in queue or queue size 4. Average delay in queue 5. Number of answering agents logged on 6. Number of answering agents unavailable to answer a call 7. Number of answering agents available to answer a call

ID Number	Name of Feature	Description
		8. Number of answering agents available to answer a call by skill 9. Longest available answering agent 10. Average speed of answer 11. Average call handling time (includes agent talk time, after-call wrap-up time and call hold time) 12. Number of calls abandoned 13. Average time to abandonment The type of network information that shall also be available to the call routing processor for utilization by the call routing logic/algorithms shall include: 1. The dialed toll-free number 2. The caller’s originating 10 digit number 3. The caller’s entered digits. Call routing logic/algorithms that shall be accommodated shall include at a minimum: 1. Routing to the best available answering agent by skill group 2. Routing based upon expected wait times 3. Routing based upon least cost. The contractor shall document the maximum hourly call processing rate and grade of service available without any degradation in performance (e.g. can process 100,000 calls per hour). The contractor shall permit the call routing processor up to 250 milliseconds from receipt of a call query to respond to the destination (or next node). In the event that 250 milliseconds are exceeded, the contractor shall route the call using a default routing plan previously defined by the ordering agency. The contractor shall provide, via a graphical user interface, all software and hardware necessary for agency access to the call routing processor to permit agency definition of the call routing logic/algorithms. The ordering agency will be responsible for providing telecommunications connections to the contractor’s system. The Network Call Distributor feature shall be offered as a managed service with the following options: 1. Contractor-provided and contractor-based: The contractor shall provide all necessary components required for the

ID Number	Name of Feature	Description
		provision of this feature and they shall be housed within the contractor's network. (Default). 2. Contractor-provided and agency-based: The contractor shall provide all necessary components required for the provision of this feature and they shall be housed at the ordering agency's designated location (Where applicable). The contractor shall provide any additional reporting or monitoring options that are available from the contractor's equivalent commercial service offering at no additional charge.
17 (Optional)	Network Queuing	The contractor shall enable TFS callers to remain, in a network queue, if resources are unavailable at the ordering agency. This is a feature that shall allow a caller to be held in queue in the contractor's network until an ordering agency's terminating SDP(s) become(s) available to receive the call. Upon entering the queue, the caller shall hear an initial announcement and shall then hear a reassurance announcement at a predetermined interval thereafter. The ordering agency shall be able to define the time for calls that can be held in queue before being sent to a terminating announcement. The contractor shall be responsible for recording announcements after ordering agency script approval.
18	NPA/NXX Routing	The contractor shall enable TFS calls to be routed to different terminations based upon the calling party's originating NPA or NPA/NXX or country code. Where NPA/NXX is not available, calls shall be routed to an agency-defined default location.
19	Percentage Call Allocation	The contractor shall enable TFS calls to be allocated on a percentage basis and terminate at multiple locations. The agency-specified percentage distribution can range from 0% to 100% in a minimum of 1% increments.
20	Real Time Reporting	The contractor shall provide agencies with the ability to monitor and report on summary and detail data relating to the status of TFS calls on a near real-time basis (e.g., minimum required refresh rate of 30 seconds and at other contractor proposed intervals). The TFS reports and monitoring data shall be available electronically within 5 minutes of the request. The contractor shall provide all components necessary to present this information in a graphical and tabular format to the ordering agency and allow it to be exported to external applications (e.g., spreadsheet or database). The user will be responsible for

ID Number	Name of Feature	Description
		providing connections to the contractor's real time monitoring system. A secure web based-interface is preferred. At a minimum, the contractor shall provide the following: 1. The number of TFS calls from each area code who have dialed a given toll free number and average call duration. 2. The total number of calls directed to an ordering agency's terminating SDP. 3. The total number of calls directed to an ordering agency's terminating SDP(s) that could and could not be completed. 4. The percentage of trunks busy at a user's terminating SDP. 5. Any standard real time reports or data available to commercial users. The contractor shall make available any reports available from its corresponding commercial service offering.
21	Routing Control	The contractor shall allow ordering agencies to perform real time and scheduled TFS call routing changes from their location or via the contractor's customer service center. This feature shall permit authorized users to review, create, validate, change, or execute call routing plans (or sets) from the ordering agency's premises or via request to the contractor's customer service center. Activation of a routing plan shall be executed in a period not to exceed 5 minutes of the request. 1. The contractor shall provide adequate security procedures that will prevent unauthorized access to this feature. 2. The contractor shall provide audit trail information to track the identity, time, and plan changes executed by a user. 3. The contractor shall provide any components necessary to enable the user to use this feature. 4. Users may provide their own terminal equipment when it meets contractor-provided specifications.
22	Service Assurance Routing	The contractor shall route TFS calls to an announcement or a predefined alternate termination within five minutes of the agency request if an emergency situation or service disruption occurs. The contractor shall complete routing requests to other types of terminations within thirty minutes of the request.
23	Speech Recognition	The contractor shall provide network based natural speech recognition applications with the ability to recognize spoken vocabulary, digits, zip codes, credit card numbers, account

ID Number	Name of Feature	Description
		numbers, alpha numeric numbers, etc. At a minimum, the contractor shall offer capabilities in (a) English, (b) Spanish and (c) (optional) other languages.
24	Tailored Call Coverage	The contractor shall enable restriction of TFS calls originating from specific areas (country, state), telephone numbers (NPA, NPA/NXX, or ANI), or call type (Payphones). The originating caller should hear a standard announcement informing them of the restriction.
25	Time of Day Routing	The contractor shall enable routing of TFS calls to different terminations or applications based upon the time-of-day. At a minimum, at least 48 time-of-day intervals shall be offered.
26	Language Interpretation Service	The contractor shall provide language translation services to support near-real time communications between callers speaking different languages.
27	Virtual Queue	The contractor shall provide a capability whereby callers can choose to remain waiting on-line for an attendant or receive a call back in turn.
28	Vanity Toll Free Number	The contractor shall provide agency-requested “vanity” toll-free numbers (e.g., 1-800-CALL-GSA), if available.

C.2.2.3.2.1 TFS Feature Reports

At the request of the ordering agency the contractor shall provide TFS reports that provide the ordering agency with information about the status of calls placed to each toll free number and/or termination. The reports shall capture this information on an (1) hourly, (2) daily, (3) weekly, (4) monthly, and (5) quarterly basis. Reports shall contain information summarized in 30- and 60-minute increments. Multiple report formats that further summarize the information by time zone or ordering agency region shall be made available where applicable. The reports shall be archived and available for a minimum of 90 days.

Reports shall be made available by electronic means such as a web site, or via e-mail or other contractor-proposed applications and have the capability to export data, in a standard file format, to agency applications (e.g., spreadsheets, databases) for analysis. The reports shall be made available electronically within 30 minutes of the submitted request. The contractor shall also provide agencies with documentation containing a description of the report, definition of the report fields, and instructions on how the agency can effectively use the report(s) to manage TFS.

All time indicators within the report shall default to Eastern Time with presentation of hours using either a 24-hour clock or a 12-hour clock with an AM/PM indicator. There shall also be an option to provide the reports indicating the time zone of the TFS terminating location.

Each report shall contain standard information including:

1. Title of Report
2. Date of Report
3. Period covered by the Report
4. Name of ordering agency
5. Toll free number(s) included in the Report

Listed below are the minimum reporting requirements. They are mandatory unless marked optional. The contractor shall also provide any historical or real-time reports that are available with its TFS reporting packages.

ID Number	Name of Feature	Description
1	Call Status Report – Toll Free Service	For any given toll free number, the contractor shall, at a minimum, provide the following information within the reports: 1. The number of call attempts from each area code and/or State that dialed the toll free number. A minimum of three views shall be available: a. calls originated by area code b. calls originated by State c. sorted by State and area code 2. The number of calls and the percentage of all calls that encounter a busy signal or that are blocked: a. Within the contractor's TFS network b. At the user's (agency's) terminating access location 3. The number of calls offered to the user TFS trunk group 4. The number of calls received at each user's terminating access

ID Number	Name of Feature	Description
		5. The number of received calls at each user's terminating access that resulted in successful answerback supervision 6.The average duration of calls answered at each user's terminating access 7. The average duration of all calls answered for a given toll free number at all terminations serving the toll free number.
2	Call Status Report – Alternate Routing	For any given toll free number utilizing Alternate Routing, the contractor shall, at a minimum, provide the following information within the reports: 1. The total number of calls offered to the initial termination 2. The number of calls that were re-routed to alternate SDP(s) or toll free service trunk group(s).
3	Call Status Report – Announcement	For any given toll free number utilizing Terminating Announcement or In-Route Announcements, the contractor shall, at a minimum, provide the following information within the reports: 1. The number of calls offered to the announcement 2. The number of calls blocked at the announcement 3. The number of calls completed in the announcement 4. The average duration of calls to each announcement 5. The number of abandoned calls for In-Route announcements.
4	Call Status Report – Call Prompter	For any given toll free number utilizing Call Prompter Access, the contractor shall, at a minimum, provide the following information within the reports: 1. The number of calls offered to the call prompter 2. The number of calls to the call prompter that were abandoned without making a selection 3. The average duration of all calls while in the call prompter 4. The number and percentage of calls selecting each option within the call prompter application.
5	Call Status Report - IVR	For any given toll free number utilizing IVR, the contractor shall, at a minimum, provide the following information within the reports by application:

ID Number	Name of Feature	Description
		1. The total number of calls offered to the IVR and average call duration 2. The number of calls completed (i.e., successfully accessed) to the IVR 3. The number and percentage of calls completed to the IVR but abandoned within the application 4. The number and percentage of calls selecting each option 5. The average duration of calls selecting each option 6. For faxback applications, the fax delivery status and usage 7. For survey applications, summary and detail information on call survey responses 8. For transcription applications, summary and detail information regarding transcription usage.
6	Caller Information Report	The contractor shall provide a report that identifies the ANI information of all callers to a specified toll free number. Note: agencies recognize that ANI, although available in most cases, is not always provided. In those instances where ANI is not available, the NPA or NPA-NXX (as available) of the caller shall be provided. Zeroes shall be substituted in place of any missing digits. For any given toll free number, the contractor shall, at a minimum, provide the following information regarding each call: 1. Date of call 2. Time of call (expressed using either a 24 hour clock or a 12 hour clock with an AM/PM indicator, Eastern Standard Time) 3. ANI of caller (if available) 4. Dialed 10 digit number 5. Duration of call 6. Disposition of call (i.e., using an alpha or numeric code) to include, at a minimum, the following information: a. Call blocked within contractor's network b. Call blocked at user's terminating access c. Call completed to user's terminating access d. Other (not included in categories a – c above)

ID Number	Name of Feature	Description
7	Caller Profile Report	The contractor shall provide the following caller information: 1. Lost Callers. The number of TFS callers who never called back after an incomplete attempt during the reporting period. 2. Average Number of Attempts Per Caller. The grand total number of call attempts divided by the number of first call attempts during the reporting period. 3. Average Number of Contacts Per Caller. The number of attempts generated from each telephone number on average during this reporting period. This is calculated by dividing the total number of first call attempts by the total number of unique telephone numbers from which the calls were made. 4. 50 Percent of Successful Attempts. Represents the number of attempts to access the network for 50 % of the callers who completed during the requested measurement interval. 5. 75 Percent of Successful Attempts. Represents the number of attempts it took to access the network for 75 % of the callers who completed during the requested interval.
8 (optional)	Call Redirection Report	The contractor shall provide a summary report on the call redirection activity by toll free number and abbreviated dial code (if applicable). At a minimum, the report should identify the following: 1. Number of transfer attempts 2. Number of completed transfers 3. Number of incomplete transfers 4. Number of blocked transfers 5. Type of call redirection (blind, supervised, or 3 way) 6. Terminating number for redirection

C.2.2.3.3 Interfaces

The UNIs at the SDP, as defined below, are mandatory unless marked optional.

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1 (Optional)	Analog Line: Two-Wire	4 kHz Bandwidth	Line-Loop Signaling

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
	(Std: Telcordia SR-TSV-002275)		
2 (Optional)	Analog Line: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Line-Loop Signaling
3	Analog Trunk: Two-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk-Loop Signaling (loop and ground start)
4	Analog Trunk: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk-E&M Signaling, Wink Start Signaling
5	Digital Trunk: T1 (Std: Telcordia SR-TSV-002275 and ANSI T1.102/107/403)	Up to 1.536 Mbps	T1 Robbed-Bit Signaling
6	Digital Trunk: ISDN PRI T Reference Point (Std: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931
7	Digital: T3 Channelized (Std: Telcordia GR-499-CORE)	Up to 43.008 Mbps	SS7, T1 Robbed-Bit Signaling
8 (Non-Domestic)	Digital Trunk: E1 Channelized (Std: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling
9 (Optional)	Optical: SONET OC-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	SS7

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
10 (Non-Domestic)	Digital: E3 Channelized (Std: ITU-TSS G.702)	Up to 30.72 Mbps	SS7, E1 Signaling
11	Digital Line: ISDN BRI S and T Reference Point (Std: ANSI T1.607 and 610)	Up to 128 Kbps (2x64 Kbps)	ITU-TSS Q.931
12	Router or LAN Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100 Mbps	SIP (IETF RFC 3261), H.323, MGCP, or SCCP

C.2.2.3.4 Performance Metrics

The performance levels and AQL of KPIs for Toll Free Service below are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Av(POP-to-POP)	Routine	99.95%	≥ 99.95%	See Note 1
Av(POP-to-terminating SDP)	Routine	99.5%	≥ 99.5%	
	Critical	99.95%	≥ 99.95%	
Grade of Service (Call Blockage)	Routine	0.07	≤ 0.07	See Note 2
	Critical	0.01	≤ 0.01	
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 3
	With Dispatch	8 hours	≤ 8 hours	

The performance metrics for TFS are based upon underlying service derived from Section C.2.2.2 Circuit Switched Voice Service.

Notes:

1. Av (POP-to-POP) and Av (POP-to-terminating SDP) are measured and calculated as a percentage of the total reporting interval time that TFS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Grade of Service (Call Blockage) is the proportion of calls that cannot be completed during the busy hour because of limits in the call handling capacity within the contractor's TFS. For example, 0.01 indicates that 1 percent of the calls are not being completed successfully (1 out of 100 calls).
3. See Section G.8.2 for the definitions and measurement guidelines.

C.2.2.4 Circuit Switched Data Service

C.2.2.4.1 Service Description

Requirements for digital connectivity on a dial-up basis will continue. The government continues to support a community of CSDS users, particularly in the area of on-demand video conferencing applications.

C.2.2.4.1.1 Functional Definition

CSDS provides a synchronous, full duplex, totally digital, circuit-switched service at multiple data rates, including integral multiples of DS0 data rates (i.e., NxDS0, where N = 1 to 24) to on-net and off-net locations.

C.2.2.4.1.2 Standards

CSDS shall comply with the following standards (as updated from time to time by the applicable governing entity):

1. ANSI X3.189
2. ITU E.721
3. Applicable Telcordia and ANSI standards for digital transmission, including SONET
4. ITU-TSS and EIA standards for DTE interfaces

C.2.2.4.1.3 Connectivity

CSDS shall connect to and interoperate with:

1. Agency-specified terminations such as Digital PBX, Intelligent MUX, Group 4 FAX, Video CODEC, and Workstation/PC
2. PSTN (where available)
3. All other EIS CSDS contractors' networks

C.2.2.4.1.4 Technical Capabilities

The following CSDS capabilities are mandatory

1. Uniform numbering plan:
    a) Unique directory number for all on-net government locations
    b) Same uniform numbering plan as proposed for VS and which shall be integrated with the VS plan (See Section C.2.2.2.1.4)
2. Authorization Codes for CSDS. Authorization codes for CSDS shall be the same as those specified for VS (see Section C.2.2.2.2 #1 and #2, Features Authorization Codes).
3. For calls terminating to off-net locations, the bandwidth requested by the originating on-net location shall be limited to the bandwidth limitations in the PSTN between the contractor's network and the called location.
4. Calling capability that does not require scheduling.
5. Provision of network-derived clocking to the DTE or PBX/Multiplexer (MUX) at the SDP.
6. Following call establishment, all bit sequences transmitted by the DTE shall be transported as data/bit transparent and shall maintain data/bit sequence integrity.
7. Categories of dialable information-payload bandwidth are as follows:
    a) DS0 Category. The dialable bandwidth shall be DS0 (i.e., 56 kbps and 64 Kbps) data rate
    b) DS1 Category. The dialable bandwidth shall be DS1 (i.e., 1.536 Mbps) data rate
    c) Multirate DS0 Category. The dialable bandwidth shall be NxDS0, where N= 1 to 24
8. For the Multirate DS0 category, the contractor shall provide the following:
    a) Appropriate dialing sequence for initiating calls with different bandwidths

b) Transport of all bit sequences transmitted by the DTE as data/bit transparent after establishment of the dialing sequence

The following categories of dialable information-payload bandwidth are optional:

1. Multirate DS1 Category. The dialable bandwidth range shall be available from DS1 to N times DS1 data rates, where N varies from 2 to 27.
2. DS3 Category. The dialable bandwidth shall be DS3 (i.e., 43.008 Mbps) data rate.
3. SONET Level-I (i.e., OC-1) Category. The dialable information-payload bandwidth shall be SONET OC-1 (i.e., 49.536 Mbps) data rate.
4. SONET Level-II (i.e., Multirate OC-1) Category. The dialable information-payload bandwidth range shall be available from SONET OC-1 to N times OC-1 data rates (concatenated), where N varies from two to three.
5. SONET Level-III (i.e., Multirate OC-3) Category. The dialable information-payload bandwidth range shall be available from SONET OC-3c to N times OC-3c data rates (concatenated), where N varies from two to four. SONET OC-3c shall support information-payload data-rate of 148.608 Mbps.

C.2.2.4.2 Features

The following CSDS features are optional:

ID Number	Name of Feature	Description
1	Dial-In	The contractor shall support toll-free numbers, in addition to 10-digit PSN numbers, for dial-in access from off-net locations (i.e., PSN) via ISDN access arrangement. Access to CSDS shall only be provided after verification of the authorization code entered by the user.
2	User-to-User Signaling Via ISDN D-Channel	User-to-user signaling via ISDN D-channel during a call shall be supported in accordance with ANSI T1 and ITU-TSS standards for ISDN and SS7.

C.2.2.4.3 Interfaces

The following UNIs at the SDP are mandatory unless marked optional:

UNI Type	Interface Type and Standards	Payload Data Rate	Signaling Type
1	ITU-TSS V.35	Up to 1.536 Mbps	RS366A (dialing)

UNI Type	Interface Type and Standards	Payload Data Rate	Signaling Type
2	EIA RS-449	Up to 1.536 Mbps	RS366A (dialing)
3	EIA RS-530	Up to 1.536 Mbps	RS366A (dialing)
4	ISDN PRI (Multirate) (T Reference Point) (Standard: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931
5	T1 (with ESF) (Std: SR-TSV-002275, and ANSI T1.102/107/403)	Up to 1.536 Mbps	SS7
6 (Optional)	T3 (Standard: Telcordia Pub GR-499-CORE)	Up to 43.008 Mbps	SS7
7 (Optional)	E1 (Standard: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling
8 (Optional)	E3 (Standard: ITU-TSS G.702)	Up to 30.72 Mbps	SS7, E1 Signaling
9 (Optional)	Optical: SONET OC-1 (Standard: ANSI T1.105 and 106)	Up to 49.536 Mbps	SS7
10 (Optional)	Electrical: SONET STS-1 (Standard: ANSI T1.105 and 106)	Up to 49.536 Mbps	SS7
11 (Optional)	SONET OC-3 (Standard: ANSI T1.105 and 106)	Up to 148.608 Mbps	SS7

UNI Type	Interface Type and Standards	Payload Data Rate	Signaling Type
12 (Optional)	SONET OC-12 (Standard: ANSI T1.105 and 106)	Up to 594.432 Mbps	SS7
13 (Optional)	ISDN BRI (Multirate) (S and T Reference Point) (Standard: ANSI T1.607 and 610)	Up to 128 Kbps	ITU-TSS Q.931

C.2.2.4.4 Performance Metrics

The performance levels and AQL of KPIs for CSDS are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability (POP-to-POP)	Routine	99.95%	≥ 99.95%	See Note 1
Availability (SDP-to-SDP)	Routine	99.5%	≥ 99.5%	
	Critical	99.95%	≥ 99.95%	
Time to Restore	With Dispatch	8 hours	≤ 8 hours	See Note 2
	Without Dispatch	4 hours	≤ 4 hours	
Grade of Service (Call Blockage)	Routine	0.07 (SDP-to-SDP)	≤0.07	See Note 3
		0.01 (POP-to-POP)	≤ 0.01	
	Critical	0.01 (SDP-to-SDP & POP-to-POP)	≤ 0.01	

Notes:

1. CSDS availability is calculated as a percentage of the total reporting interval time that CSDS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Refer to Section G.8.2 for definition and how to measure.
3. Grade of Service (Call Blockage) is the proportion of calls that cannot be completed during the busy hour because of limits in the call handling capacity of one or more network elements (e.g., “All trunks busy” condition). For example, 0.01 indicates that 1 percent of the calls are not being completed (1 out of 100 calls).

C.2.3 Contact Center Service

C.2.3.1 Service Description

Contact Center Service (CCS) provides services and personnel to enable agencies to deliver customer service to their clientele across multiple contact channels (voice, fax, email, Internet web site, SMS, chat, etc.) by providing a single network call queue or multiple call queues (where applicable). A network call queue manages multimedia customer interactions such as voice, email, web submissions, and fax. The call queue(s) provides the consistent, real-time management and distribution of multi-media calls to an agency contact center. CCS may be used in conjunction with toll-free and other network services to facilitate agency communications with the general public, businesses, and other agencies. CCS also offers a call answering service with the call queue. The CCS call answering service enables the agency to use contractor-provided resources to respond to caller inquiries. The contractor-provided call answering resources can be located at either 1) an agency location(s) or 2) a contractor location(s).

C.2.3.1.1 Functional Definition

CCS can enable ordering agencies to deliver customer service to their designated customer base across multi-media contact channels (voice, fax, email, web site, etc.) and provide additional enabling services for end-to-end customer service. The basic service provides intelligent call routing capabilities with a network call queue. CCS will apply to single site, multiple site, and enterprise-wide agency contact centers.

C.2.3.1.2 Standards

The following CCS standards are mandatory unless marked optional:

1. (Optional) Computer Supported Telephony Applications (CSTA)
2. IETF RFC’s for IPv4 and IPv6

3. ITU-T H.248.1 / Megaco (IETF RFC 3525)
4. ITU-T H.323
5. ITU-T T.30, T.37, T.38, and T.120
6. (Optional) Skinny Client Control Protocol (SCCP)
7. IETF RFC 3261 for Session Initiation Protocol (SIP)
8. Voice eXtensible Markup Language (VxML)
9. All appropriate standards for any underlying access and transport services.

The contractor shall comply with all new versions, amendments, and modifications made to the above listed documents and standards.

C.2.3.1.3 Connectivity

CCS shall connect and interoperate with PSTN.

C.2.3.1.4 Technical Capabilities

The following CCS capabilities are mandatory unless marked optional:

C.2.3.1.4.1 CCS Delivery Methods

The contractor shall provide the following independent service delivery methods for CCS:

1. **Host Based Call Management Service**. The contractor shall provide the necessary components required for CCS Call Management Service at a contractor-provided location. This includes, but is not limited to, hardware, software, inside wiring, and power.
2. **Premises Based Call Management Service**. The contractor shall provide the necessary components required for CCS Call Management Service to be located at an agency-provided location. This includes, but is not limited to, CCS hardware and software. The contractor shall install, configure, and maintain the CCS equipment. The agency will provide the power, inside wiring, and a physical location for the contractor's CCS equipment.
3. **Premises Based Call Answering Service**. The contractor-provided personnel shall perform operations at an agency-provided location. The agency will provide the work space, furniture, workstation hardware, software, and all necessary building utilities required for the contact center.
4. **Host Based Call Answering Service**. The contractor personnel shall be located and perform operations at a contractor-provided location. The contractor shall provide the work space, furniture, workstation hardware, software, and all necessary building utilities for the contact center.

C.2.3.1.4.2 CCS Call Management Service

1. The contractor shall provide the capability for a network call queue (a single queue or multiple queues according to agency needs) to manage the routing and distribution of contacts (calls) from multi-media channels such as voice, email, facsimile, and an agency web site.
2. The intelligent routing and distribution of contacts shall be determined according to the real time operating status of the ordering agency's contact center(s) and its business rules. The agency business rules can be based upon parameters such as media type, real time status of the contact center, caller profile, call content, and agent skills. The contractor shall provide the capability to prioritize queues and contacts (calls) within a queue.
3. The contractor's CCS shall interoperate with the ordering agency's CCS communications channels such as the web site, e-mail, voice, fax and chat (when applicable).
4. The contractor's CCS shall have the capability to traverse and successfully interoperate with agency firewalls and security layers. The contractor shall verify with the agency that the agency firewall is compatible with the service.
5. The contractor shall support service observation, which provides agency authorized personnel with the capability to monitor the CCS trunks, agents, and agent groups for call quality. The contractor shall provide options for silent monitoring (default) and three-way audio conferencing. Service observation shall be made available for monitoring both local and remote agents and support local and remote observers. Service observation shall be secure and available only to authorized agency-designated individuals.
6. The contractor shall provide the ordering agency with the capability to manage its specific network queue, call routing algorithms, contact center agent profiles, and reports. The CCS shall enable authorized agency designated individuals to perform both real time and scheduled changes. The CCS management system shall provide the following minimum administrative capabilities:
   a) An audit trail and change log history
   b) Authentication with password protection for authorized administrators
   c) Ability to perform scheduled and real-time changes
   d) Ability to view the agency CCS configuration
7. The contractor shall provide reports as required by the OCO.
8. The contractor shall provide the ordering agency with access to graphical, real time reporting of the CCS queue status. The real time reporting shall monitor performance and identify all interactions (voice, email, fax, web and chat) by contact channel and agent status. The reports shall include summaries and totals

(where applicable). The real time reporting shall provide the following minimum capabilities:

a) Number of inbound contacts (calls)
b) Status of inbound contacts (calls)
c) Number of contacts (calls) in queue
d) Length of oldest contact (call) in queue
e) Average queue time
f) Number of abandon calls
g) Agent status and performance statistics
h) Service level information
i) Number of contacts handled by workgroup or skill

9. The contractor shall provide the capability to inform the caller of the queue status including the callers estimated wait time in queue when a queue threshold exceeds an agency defined threshold. This can also include an option for announcing the caller’s expected wait time prior to entering the queue. The contractor shall provide agencies with the ability to change recorded announcements.
10. The contractor shall provide the capability to transmit and deliver music on hold (or recordings) to the originating caller. The music on hold source can be contractor or agency provided according to the ordering agency’s needs.
11. The contractor shall supply terminal devices (e.g., phones, IP phones, softphones) required for delivery of CCS if requested by the ordering agency. Terminals shall have the capability to support caller ID and an optional name/message display (where applicable).
12. The contractor shall provide the capability to accommodate agency contact center closings (e.g., scheduled holidays, unplanned closings, outside of normal business hours, and closings for maintenance activities) by providing announcements, messages, or re-routing of contacts during the period when the agency contact center is closed.

C.2.3.1.4.3 CCS Call Answering Service

1. The contractor shall provide a CCS Call Answering Service. The contractor shall provide agencies with a contact center operation, which may include network services, technology, personnel, business processes and workflows, training, and reporting to respond to caller inquiries and meet pre-determined performance or customer satisfaction levels.
2. The contractor shall meet the following CCS Call Answering Service requirements:
   a) The contractor shall receive and accurately respond to caller inquiries during established agency operating hours within the agreed-upon KPIs.

b) The contractor shall manage and accurately respond to caller inquiries received during non-operational hours and holidays according to the ordering agency's needs.

c) The CCS shall be interoperable with the ordering agencies' required back office systems or databases (if required and as identified by the agency) to deliver the specified customer service functions at the agreed-upon performance levels.

d) The contractor shall provide resources, processes, and technology to reasonably accommodate inquiries from different types of callers as identified by the ordering agency. This shall include responding to inquiries from callers that may have foreign language requirements or callers with disabilities including but not limited to speech disabilities, deaf, hard-of-hearing, deaf/blind, or blind (e.g., support TDD/TTY calls).

e) The contractor shall provide a description of its capability to quickly increase capacity in crisis or high-priority situations. The contractor shall quantify its ability to deliver call answer services in terms of capacity, extended operating hours, increased staffing, additional language support and implementation start-up time.

3. The contractor shall provide call answering resources, as needed, in order to meet the requirements specified in the agency service order, according to the descriptions listed in Table C.2.3.1.4.4 below:

C.2.3.1.4.4 CCS Call Answering Resources Table

Role	Description
Basic Call Answering	1. Receive inbound calls and respond to caller inquiries 2. Question callers to obtain full understanding of what information is being requested. 3. Document all customer contacts 4. Follow contact center operational procedures 5. English language proficiency required

C.2.3.1.5 Features

The following CCS features are mandatory unless marked optional.

ID Number	Name of Feature	Description
1	Call Recording and Monitoring	The contractor shall provide digital recording and monitoring of inbound and outgoing multimedia contacts (telephone, email, and web self-service channels) and associated data (agent screen capture) to capture the caller experience. At a minimum, the date, time, duration,

ID Number	Name of Feature	Description
		caller ID information (if available), dialogue, and identity of the agent handling the call shall be captured and recorded. Archived calls shall be able to be retrieved by date, time, agent, content, contact channel, or identity of the caller. The following minimum capabilities shall be provided: 1. Archive recordings 2. Playback of recording 3. Provide the capability for the recording of an agent to be activated and de-activated on demand. 4. Remote monitoring and playback 5. Reporting (management and administrative) 6. Programmable scheduled and random call recording 7. Selective recording (based on business rules) 8. Support free seating 9. Total and random recording of all calls 10. Convert call recordings to .wav or mp3 file format The call monitoring system shall also provide the capability for evaluating and scoring calls and performing random call quality reviews.
2	Collaborative Browsing	This contractor shall allow bi-directional sharing of web pages between the contract center agent and the caller. It shall enable a caller to request a co-browse session with a contact center agent. The agent shall have the capability to highlight text and scroll the browser screen to a specific section of a web page. The agent shall have the capability to push a web page to the caller and vice-versa. The contractor shall allow the capability for an agent to transfer control of a collaborative browsing session to another agent and log all collaborative interactions between the agent and caller. The contractor shall state if there are any restrictions or limitations regarding the type of web browser software used by the caller or contact center agent for use with this feature. The contractor shall provide the ability to mask fields and inputs of private/sensitive information.
3	Computer Telephony Integration (CTI)	The contractor shall provide Computer Telephony Integration (CTI) capability to enable transfer of caller information and agency specified data between the contractor and agency specified systems simultaneously with the associated inbound contact channel (call). This feature can be used to support a diverse set of agency applications such as screen pop/splash, intelligent routing, third party call control, keyboard dialing, enhanced reporting, and multi-channel call blending solutions.
4	Customer Contact Application	The contractor shall provide an application to track, document, and manage the CCS customer contacts across multiple contact channels. The customer contact

ID Number	Name of Feature	Description
		application shall contain the following minimum capabilities: 1. Record caller contact information 2. Record caller account information 3. Record caller contact history and status of inquiry 4. Record nature of the inquiry 5. Record date and time of the contact 6. Record call disposition 7. Record agent handling the inquiry 8. Assign & escalate inquiries according to business rules 9. Assign a unique case or record number to each inquiry The customer contact application shall also provide the capability to create and provide scripted responses for the contact center agents. The contact system shall also provide summary and detailed management reports.
5	E-mail Response Management	The contractor shall provide E-mail Response Management (ERM) that shall assign a tracking ID to each email and route e-mail communication according to agency specified business rules. The ERM shall provide the following minimum capabilities: 1. Auto response 2. Automatic acknowledgement 3. Email classification and prioritization 4. Email routing based upon business rules 5. Filtering capability 6. Content analysis and knowledge base for suggested and personalized responses 7. Management reports 8. Multiple language support (English and Spanish) 9. Real time exception reports The ERM shall be compatible with the ordering agency's e-mail application.
6	Interactive Voice Response (IVR)	The contractor shall provide an interactive voice response application that allows callers to be provided with information based upon input from (a) telephone DTMF key pad entries or via (b) speech recognition. The minimum capabilities are listed below: 1. Select pre-recorded announcement messages with the capability for announcements and provide the ability for a caller to opt out during an announcement to a predefined termination. Such announcements shall always be played from the beginning for each caller and provide the capability to be recorded in (a) U.S. English, (b) Spanish (American) and (c) other foreign languages after obtaining ordering agency script approval.

ID Number	Name of Feature	Description
		2. Leave caller information via telephone DTMF keypad signal or speech (e.g., name, address, account information, etc.). 3. A means for the ordering agency to retrieve caller-entered DTMF or speech messages. 4. For transcription of caller information, the contractor shall provide (a) transmission of the recorded voice files and DTMF data for each call to the agency and (b) a report of caller responses that transcribes the caller-provided information for the ordering agency based upon the agency's needs and transmits it to the agency. The contractor shall provide transcription reports from English- and Spanish-speaking callers. 5. Query a database that delivers agency-provided information to the caller. The database may be housed in the (a) ordering agency or, at the ordering agency's discretion, (b) housed in a contractor location and updated by the ordering agency. Provide a default routing or message (agency option) if the database is unavailable. 6. Provide a capability to allow callers to hear and verify their names and addresses in an agency-provided name and address database after the caller has entered his or her telephone number via DTMF, or based on the caller's ANI. (Text to Speech). 7. Support speech recognition as a valid caller input. The contractor shall support at a minimum, all spoken numeric digits as well as "yes" and "no." English and Spanish language callers shall be supported. The contractor shall be able to accept and process at a minimum 95 percent of the above speech responses. The speech responses which are not accepted shall be routed to default location designated by the ordering agency. 8. Provide the capability to perform surveys (via DTMF or speech) to IVR callers. The surveys can be provided to all or a random percentage of callers according to agency needs. Survey results shall be provided electronically to the ordering agency. 9. Provide a facsimile "fax back" capability (Fax or equivalent) that shall permit callers to retrieve agency-specific documents or forms. The contractor shall fax back the request documents within one hour of the initial call and retry a minimum of 13 attempts over a six hour interval in order to complete the request. Fax transmittal shall include an option for a cover sheet (standard or customized). 10. At the agency's option, the caller's IVR selection(s) information shall be transferred to the agency.

ID Number	Name of Feature	Description
		11. The contractor's IVR capacity must be configured such that the application answers a call within 3 ring cycles for 99 % of the offered call volume (measured on an hourly basis). 12. Features equivalent to the above shall be available to individuals who are hearing impaired or have speech disabilities via electronic means in Baudot and ASCII/TTY code formats. These electronic form lines need not be voice feature enabled. 13. The contractor shall provide summary reporting that at a minimum provides information on the caller, average call duration, caller opt out (transfer) and disposition of the calls within the IVR application on a daily, weekly and monthly basis. 14. The contractor shall make available any IVR reports that are available with its equivalent commercial offerings
7	IVR - Agency Based Database (Host Connect)	The contractor shall provide the ability to route calls or provide information based upon a database query(s) of information provided by a database located at the ordering agency premises. The query(s) could be to single, redundant, or multiple databases depending upon agency specifications and the complexity of the application. The contractor shall implement and provide the appropriate interface and connectivity for the contractor's IVR application to successfully query and access the ordering agency's database(s). The IVR caller shall have the capability to retrieve, review, and modify information located on the agency based database based upon the ordering agency's needs. The agency database(s) can be a (a) mainframe or (b) server based relational database. If the database does not respond to the network query within 250 milliseconds, an agency defined default routing plan shall be used.
8	Reserved	
9	IVR - Speech Recognition	The contractor shall provide natural speech recognition for IVR applications with the ability, at a minimum, to recognize spoken vocabulary, digits, zip codes, credit card numbers, credit card expiration date, account numbers, alpha numeric numbers. At a minimum the contractor shall provide natural speech recognition capabilities and vocabularies for both English (American) and Spanish (American) dialects. The minimum accuracy threshold for speech recognition shall be at least 95%.
10	Language Interpretation Service	The contractor shall provide telephone language interpretation services. The service should be available, on demand, for three way conferencing with the contact center agent and foreign language caller to provide

ID Number	Name of Feature	Description
		interpretation between the caller's foreign language and English and vice versa. This feature shall have the following minimum capabilities: 1. Available 24x7 2. Accessible via a toll free number 3. Identify the foreign language of the caller 4. Provide an appropriate interpreter within one minute of the request 5. Provide management reports identifying the date, time, duration, interpreter, and identity of the agent requesting the service. The contractor shall propose and provide a list of the foreign languages available for interpretation. Spanish is a mandatory language.
11	Outbound Dialer	The contractor shall provide the capability for automated outbound dialing. The dialer service shall have the capability to support either centralized or distributed contact center environments according to the ordering agency's needs. The dialer shall have the following minimum capabilities: 1. Automatically initiate domestic and non-domestic outbound calls 2. Call conferencing and call transfer capability 3. Predictive dialing - capture real-time statistics from the call queue and automatically adjusting the outbound dialing frequency according to agency defined service level parameters 4. Preview dialing - allow agents to preview the customer record before an outbound call is initiated and provide an option for the agent to cancel the call 5. Receive and manage inbound calls 6. Support agent blending. The integration of outbound and inbound call handling to determine how to best use agent resources. (agents can handle both outbound and inbound calls) 7. Support service observation 8. Reporting – Provide comprehensive historical, real time management, and exception reports.
12	Text Chat (Web Chat)	The contractor shall provide the ability to enable the contact center agents to engage in real time text chat with callers directed from its web site. The text chat shall provide the following minimum capabilities: 1. Archive text chat sessions (create transcripts) 2. Allow agents to manage multiple text chat sessions 3. Allow file transfers 4. View the active web page the text chat caller is on 5. Provide a log of text chat sessions 6. Provide an automatic spell check and grammar check option that is enabled when typing in active session.

ID Number	Name of Feature	Description
		7. Supervisor chat monitoring
13	Web Call Back	The contractor shall provide the capability for a customer to request a call back by filling out a form on the agency's web site. The call back algorithm shall be based upon the availability of a contact center agent. The call back request shall be automatically distributed to the most appropriate agent based upon availability of an agent (within agency operating hours).
14	Web Call Through	The contractor shall provide the capability to enable customers browsing the agency's web site the ability to call through (e.g. "click to talk") and simultaneously have a voice conversation with a contact center agent.
15	Workforce Management	The contractor shall provide a workforce management (WFM) system that automates forecasting and scheduling calculations based upon real time and historical contact center data. The WFM shall enable agencies to effectively schedule resources, accurately forecast call volumes and analyze/review performance statistics for single or multiple sites and blended applications. The workforce management system should provide the following minimum capabilities: 1. Forecast staffing needs including agent skills, skill levels and shifts. 2. Forecast contact volumes and workload - overall call volume and by contact channel. 3. Provide agent scheduling and create optimized agent schedules by shift and skill.
16	Virtual Queue	The contractor shall provide a capability whereby callers can choose to remain waiting on-line for an attendant or receive a call back in turn.

C.2.3.1.6 Interfaces

CCS is an application layer service which uses underlying network service(s) to deliver customer service capabilities. Where applicable, refer to the interface requirement sections below:

1. Section C.2.2 Voice Service
2. Section C.2.4 Colocated Hosting Service

C.2.3.1.7 Performance Metrics

The performance levels and AQL of KPIs for CCS are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
	Critical	99.9%	≥ 99.9%	
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 2
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Availability is measured and calculated as a percentage of the total reporting interval time that CCS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section G.8.2 for the definitions and measurement guidelines.

C.2.4 Colocated Hosting Service

There may be requirements for the contractor to provide facilities for a data center that will be populated by GFP, such as servers, routers and load balancers.

C.2.4.1 Functional Definition

Colocated Hosting Service (CHS) shall provide a secure location with cage and racks and include site surveillance. This service also provides external traffic access as required; Internet and other dedicated connection (e.g., PLS and ETS) speeds, space requirements, maintenance support and operational support will be specified in TOs.

The contractor shall provide the government and its representatives with 24x7 access to leased space and GFP in the co-location facility. The co-location facility shall support the following capabilities:

1. Redundant and high-availability power to GFP.
2. Redundant Uninterruptible Power Supplies (UPS). UPS systems shall receive power both from commercial power feeders and alternate power sources.

3. A Very Early Smoke Detection Apparatus (VESDA) system shall be provided for fire detection.
4. A fire suppression system shall be provided. Acceptable systems include (but are not limited to) multi-zone, pre-action, dry pipe systems.
5. Redundant cooling systems.

C.2.4.2 Standards

CHS shall comply with the following standards:

1. TIA-942 Telecommunications Infrastructure Standard for Data Centers (as updated)
2. NIST SP800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations
3. ICD 705, 26 May 2010, Sensitive Compartmented Information Facilities (as required)

C.2.4.3 Connectivity

CHS shall provide external connectivity as required in accordance with the TO.

C.2.4.4 Technical Capabilities

CHS requires the following mandatory capabilities:

1. At the contractor’s facility, the contractor shall be responsible for the following, as required:
   a) Assuming responsibility for all damage or injury to persons or property occasioned through the use, maintenance, management, and operation of the contractor’s facilities, GFP, or other equipment by, or by the action of, the contractor or contractor’s employees and agents. The government shall in no event be liable or responsible for damage or injury to any person or property occasioned through the use, maintenance, management, or operation of any facility, GFP, or other equipment by, or by the action of, the contractor or the contractor’s employees and agents in performing under this contract, and the Government shall be indemnified against claims for damage or injury in such cases.
   b) Completing any necessary pre-delivery preparations for the delivery site, site security, or storage facilities to temporarily or permanently accommodate the GFP in a safe and secure manner.
   c) Relocating GFP from initial receiving points or temporary storage facilities to the final contractor facility and installation site.

d) Preparing the final installation site including the provisioning of necessary physical space, environmental systems, and network connectivity, including but not limited to: Internet working connections, fire suppression, HVAC, power, lighting, water, sewer, telephone and communications, physical security systems, network security systems, disaster resistance and recovery systems, cages, racks, and UPS, emergency power systems, all on a 24x7 basis, unless otherwise mutually agreed upon and specified.

e) Facilitating GFP setup, including assembling, loading, configuring, testing, and (at end of life) crating and packing GFP for return. Determinations of inter-compatibility and inter-operability shall be conducted by the contractor as soon as practical after delivery and setup.

f) Providing contractor personnel with all required national citizenship, security clearances, training, and technical certifications to receive, use, maintain, manage, operate, package, transport, or ship sensitive and secure GFP.

2. Authorized government personnel and third-parties shall have access to GFP at specified times, in specified locations, as mutually agreed upon between the government and the contractor. Government personnel shall conform to the contractor's Acceptable Use Policy (AUP) in effect at the specified contractor facility, except where the AUP conflicts with government policy, or other government executive orders, regulations or laws.
3. The contractor shall provide a service management capability such that user can remotely monitor facility and equipment status in real-time.
4. The service management capability shall present alarms to the user in real-time for facility and communication failures.
5. The service management capability shall continuously update and present to the user the status of power for each rack, cooling, environment temperature, entry/exit logs, smoke detection, and connectivity.

C.2.4.5 Features

The contractor may be required to provide CHS in an Intelligence Community Directive (ICD) 705 Sensitive Compartmented Information Facility (SCIF). The size and other characteristics of a SCIF will be provided in the TO.

C.2.4.5.1 Performance Metrics

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Internet Availability	Critical	99.99%	≥ 99.99%	See Note 1

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 2

Notes:

1. Availability is measured and calculated as a percentage of the total reporting interval time that CCS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. See Section G.8.2 for the definitions and measurement guidelines.

C.2.5 Cloud Service

NIST SP 800-145 defines cloud services as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). All cloud services offered shall be FedRAMP certified. The contractor shall support the five essential characteristics and four deployment models of cloud services defined in NIST SP 800-145 and listed below.

Essential characteristics:

1. On Demand Self-Service – ability to select and provision services as needed
2. Broad Network Access – universal access to thin or thick client platforms such as mobile devices, laptops, and PDAs
3. Location Independent Resource Pooling – computing resources are shared, serving multiple consumers
4. Rapid Elasticity – ability to immediately scale up or down based on user needs and peak demands
5. Measured Service – ability to pay only for what is used

Deployment Models:

1. Private cloud – generally controlled, managed, and hosted by a single organization
2. Community cloud – same as Private cloud except that the cloud is shared by multiple organizations (e.g., federal agencies or sub-agencies) with similar security and performance goals

3. Public cloud – different users share infrastructure and receive a standardized, yet highly scalable, type of capacity
4. Hybrid cloud – combination of at least one Private cloud and one Public cloud connected to allow programs and data to be easily shared. This allows an organization, for example, the ability to burst fluctuating workloads into the public cloud when necessary.

The deployment of cloud services in the Federal Government is mandated by the OMB's "Cloud First" policy for any federal IT acquisition, the Federal Cloud Computing Initiative (FCCI) by the Federal CIO Council for government cloud computing framework and requirements, and FedRAMP for a unified risk management framework for cloud computing.

In accordance with the NIST and Federal mandates and requirements, the contractor shall support cloud services (IaaS, PaaS, and SaaS in any combination) as described in the following sub-sections.

C.2.5.1 Infrastructure as a Service

C.2.5.1.1 Service Description

The contractor shall provide a solution for provisioning required computing and networking resources and supporting the FedRAMP and TIC overlay requirements.

IaaS shall be composed of the following subservices: 1) Private Cloud IaaS and 2) Data Center Augmentation with Common IT Service Management (ITSM). These subservices are described in the following subsections.

C.2.5.1.1.1 Functional Definition

The Private Cloud IaaS subservice shall offer a private cloud IaaS solution that includes virtual machines, storage, and server hosting. The cloud platform provides necessary network infrastructure (e.g., LAN, load balancer, and firewall), security components, storage backup, continuity of operation, and disaster recovery services. The private cloud may be either an "air-gapped Private Cloud" where the cloud platform is based on physical infrastructure dedicated to the customer agency, or a "virtual-gapped Community Cloud" where the cloud platform physical infrastructure is shared by two or more agencies and the allocated virtual resources are separated by an agency-specific security envelope/perimeter.

The Data Center Augmentation with Common ITSM subservice shall enable augmentation of already-virtualized agency premises data center resources with dynamically expandable and contractible virtualized cloud-based resources. This service includes a common IT management framework for agency data center resources and cloud resources. The common ITSM framework for data center resources will allow data center managers to follow the same processes for managing the additional cloud resources that they use to manage their data center resources.

C.2.5.1.1.2 Standards

IaaS shall comply with the following standards:

1. NIST:
    a) NIST SP 800-145 "The NIST Definition of Cloud Computing," September 2011
    b) NIST SP 500-292 "NIST Cloud Computing Reference Architecture," September 2011
    c) NIST SP 800-53 (rev.4) "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013
    d) NIST SP 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," April 2010
    e) NIST SP 800-46 (rev.1) “Guide to Enterprise Telework and Remote Access Security”
    f) NIST SP 800-171 “Protecting Controlled Unclassified Information in the Nonfederal Information Systems and Organizations,” June 2015
2. ITIL: ITILv3
3. SNMP: SNMPv3
4. FedRAMP TIC Overlay; see https://www.fedramp.gov/files/2015/04/Description-FT-Overlay.docx
5. OMB M-06-16 "Protection of Sensitive Agency Information," 23 June 2006
6. ISO 17203 “Open Virtualization Format Specification”
7. FIPS 140-2, Security Requirements for Cryptographic Modules
8. FIPS 140-3, Security Requirements for Cryptographic Modules
9. FIPS 197, Advanced Encryption Standard
10. DOD STD-5015.2 V3, Electronic Records Management Software Applications Design Criteria Standard
11. NARA Bulletin 2008-05, July 31, 2008, Guidance concerning the use of e-mail archiving applications to store e-mail
12. NARA Bulletin 2010-05, September 08, 2010, Guidance on Managing Records in Cloud Computing Environments

C.2.5.1.1.3 Connectivity

Network connectivity from agency sites to the contractor's cloud services shall be supported through communications services offered through this contract as appropriate.

C.2.5.1.1.4 Technical Capabilities

C.2.5.1.1.4.1 Technical Capabilities of Private Cloud

The contract shall support the basic capabilities for Private Cloud IaaS defined in NIST SP 800-145 as specified in the TO. These capabilities are mandatory unless marked optional:

1. Access to agency data in data centers shall comply with National Policy as defined in C.1.8.8 including agency sites and remote locations.
2. Cloud Data Center Security:
   a) Provide secure connectivity among contractor's data centers for elasticity (expansion and contraction) of computing resources
   b) Secure connectivity to contractor's data center from agency sites
   c) Provide additional compliance and certification requirements as specified in the TO
3. Agency Cloud Service Security
   a) Create and maintain a security perimeter around an agency's data and VMs
   b) Data-at-rest encryption in accordance with FIPS 197
4. Virtualized elastic computing infrastructure:
   a) Virtual Machines (VMs)
   b) Network Storage
5. Server Hosting
   a) Private-facing Internal Web Hosting
   b) Public-facing External Web Hosting
6. Backup and Restore agency data
7. On-demand self-service IaaS provisioning, configuration management, topology management, security management, activation and deactivation via portal scripting language or API with role based access control for portal login which is OMB M-11-11 compliant
8. Visibility into usage of measured/metered (usage-based) service.
9. Allow users to have VMs with their own private IP address blocks.
10. Support bulk import and export of VM per ISO 17203.

11. Allow users access to log events such as resource provisioning and de-provisioning, VM start and stop, and account changes, for at least 60 days.
12. (Optional) Allow users to place metadata tags on provisioned resources and to run reports based on them, which is useful for internal showback or chargeback.
13. Support cost control measures such as quotas (limits on what a user can provision) and leases (time-limited provisioning of resources).
14. Support with 24x7 customer service, via phone, email and chat.
15. The agency retains exclusive ownership over all of its data in the cloud. The contractor shall provide tools to allow the client agency to fully retrieve its data in the original or a mutually agreed-upon format.
16. Cloud resources, particularly the data at rest, must be located within the U.S. or the jurisdiction identified in the TO to allow electronic discovery (eDiscovery) of identification, collection, processing, forensic analysis, auditing, and production of Electronically Stored Information (ESI) required in the discovery phase of litigation. This shall also include government access to the contractor's cloud data center facilities, installations, technical capabilities, operations, documentation, records, and databases if required. See Section H.33 for additional eDiscovery requirements.
17. The contractor shall provide Disaster Recovery (DR) and Continuity of Operations (COOP) per agency-specific requirements in the TO.

C.2.5.1.1.4.2 Technical Capabilities of Data Center Augmentation with Common Information Technology Service Management

The contractor shall support the following technical capabilities for Data Center Augmentation with Common ITSM. The following capabilities are mandatory unless marked optional:

1. Ability to manage both cloud virtual resources and the agency data center's virtual resources with interoperable monitoring and control capabilities.
2. The contractor's management platform shall include a visual indicator of which resources are in the cloud and which are premises resources.
3. (Optional) Ability to integrate with agency's data center management platform.

C.2.5.1.2 Features

The following features are mandatory unless marked optional:

1. (Optional) "Bare metal" physical servers: Ability to have "bare metal" physical servers on a dynamic basis with provisioning times of two hours or less. This capability may be required for (a) a large-scale database requiring an incremental storage capacity, or (b) specialized network equipment that may

not be available in the cloud, or (c) software that cannot be licensed on virtualized servers, or (d) legacy equipment that cannot be virtualized, or (e) agencies that plan to move into collocation first and then gradually migrate into the provider's cloud.

2. Data management and analytics: This capability shall complement and extend log management and analysis services and other data center management services, per agency-specific requirements in the TO.

C.2.5.1.3 Interfaces

The contractor shall support the interfaces identified in the TO.

C.2.5.1.4 Performance Metrics

The performance levels and AQL of KPIs for the contractor's IaaS cloud service are defined below. In addition, the contractor shall meet service level objectives for performance, privacy, security and support as specified in the TO.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability (IaaS cloud service)	Routine	99.95%	≥ 99.95%	See Note 1
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. IaaS cloud service Infrastructure availability is calculated as a percentage of the total reporting interval time that the IaaS infrastructure is operationally available to the agency. Availability is computed by the standard formula:

$$Av(IaaS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$
.

The scheduled maintenance windows are excluded from the availability calculation.

C.2.5.2 Platform as a Service

C.2.5.2.1 Service Description

C.2.5.2.1.1 Functional Definition

PaaS provides the capability for the user to deploy and employ applications using software tools supported by the cloud provider.

C.2.5.2.1.2 Standards

Same as specified for IaaS. See Section C.2.5.1.1.2 for details.

C.2.5.2.1.3 Connectivity

Same as specified for IaaS. See Section C.2.5.1.1.3 for details.

C.2.5.2.1.4 Technical Capabilities

The contractor shall provide the following PaaS capabilities including, but not limited to:

1. Access to agency data in data centers shall comply with National Policy as defined in C.1.8.8 including agency sites and remote locations.
2. Developer Tools:
   a) Integrated Development Environment (IDE) Suite
   b) Application Server
   c) Utilities/Libraries
3. Database Systems (DBMS/RDMS)
4. Big Data Solution Platform
5. Directory, based on, but not limited to, LDAP/X.500 based implementations, to support directory schemas, defined as object classes, attributes, name bindings, and knowledge (namespaces)
6. Testing Tools:
   a) Application Test Tools
   b) Web Test Tools
   c) Workflow Tools

The agency retains exclusive ownership over all of its data in the cloud. The contractor shall provide tools to allow the client agency to fully access PaaS-related data from the cloud in a usable format as needed.

C.2.5.2.2 Features

None.

C.2.5.2.3 Interfaces

The contractor shall support the interfaces identified in the TO.

C.2.5.2.4 Performance Metrics

The contractor shall meet PaaS cloud service KPIs. See Section C.2.5.1.4 for details.

In addition, the contractor shall meet service level objectives for performance, privacy, security and support as specified in the TO.

C.2.5.3 Software as a Service

C.2.5.3.1 Service Description

C.2.5.3.1.1 Functional Definition

Software as a Service (SaaS) allows software and applications to be hosted in the cloud and accessed by users via, for example, agency intranet.

C.2.5.3.1.2 Standards

Same as specified for IaaS. See Section C.2.5.1.1.2 for details.

C.2.5.3.1.3 Connectivity

Same as specified for IaaS. See Section C.2.5.1.1.3 for details.

C.2.5.3.1.4 Technical Capabilities

The contractor shall provide the following SaaS capabilities including, but not limited to:

1. Access to agency data in data centers shall comply with National Policy as defined in C.1.8.8 including agency sites and remote locations.
2. Customer Relationship Management (CRM) tools
3. Enterprise Resource Planning (ERP) tools
4. Human Capital Management (HCM) tools
5. Desktop applications
6. Office automation tools
7. Security tools
8. Others as defined in the TO

The agency retains exclusive ownership over all of its data in the cloud. The contractor shall provide tools to allow the client agency to fully access SaaS-related data from the cloud in usable format as needed.

C.2.5.3.2 Features

None.

C.2.5.3.3 Interfaces

The contractor shall provide the following UNIs:

1. The contractor shall support the interfaces identified in the TO.
2. Platform-specific API or client software to connect to the cloud SaaS platform.

C.2.5.3.4 Performance Metrics

The contractor shall comply with the following performance metrics:

1. Same as specified for IaaS. See Section C.2.5.1.4 for details.
2. Most current software release with all the patches applied or as specified in the TO.

C.2.5.4 Content Delivery Network Service

C.2.5.4.1 Service Description

Content Delivery Network Service (CDNS) delivers agency content to Web browsers worldwide. The CDNS provider incorporates equipment and algorithms to cache content on geographically dispersed servers on the Internet. When a request is made from a particular location for specific content, the server that can most rapidly and efficiently provide the content is dynamically identified.

C.2.5.4.1.1 Functional Definition

A Content Delivery Network (CDN) consists of a collection of surrogate servers that attempt to offload work from origin servers by delivering content on their behalf. The servers belonging to a CDNS may be located at the same site as the origin server, or at different locations around the network, with some or all of the origin server's content cached or replicated among the CDNS servers. For each request, the CDNS attempts to locate a CDN server close to the client agency to serve the request, where "close" could include geographical, topological, or latency considerations.

CDNS addresses the following technical and operational issues:

- Latency – the delay in delivering Web content to the end-user
- Scalability – Web services automatically scale up as end-user requests increase
- Reliability – content is always available and its integrity is assured (i.e., has not been altered by third parties including hackers)

- Flash crowd control – i.e., effectively meeting demand during periods of unexpected high usage

C.2.5.4.1.2 Standards

CDNS shall comply with the following standards:

1. Hyper Text Transfer Protocol (HTTP)
2. IETF – Request for Comments
3. Transport Layer Security (TLS)

The contractor shall comply with new versions, amendments, and modifications made to the above listed documents/standards.

C.2.5.4.1.3 Connectivity

CDNS shall connect to and interoperate with the following:

1. Internet for content distribution to public
2. IP network (agency-owned or contractor-provided) for loading and administration of web server by the agency

C.2.5.4.1.4 Technical Capabilities

The following CDNS capabilities are mandatory unless marked optional:

1. Content Distribution:
    a) Static Content Download Service:
        i. This service provides fast, secure, and reliable download of content including text, video and music. Such content will likely be stored on CDNS servers that are deployed globally.
    b) Real-time Streaming (Webcasting):
        i. The contractor shall deliver streams in real time (the CDNS shall encode the signal when sent in raw signal format by the content provider).
        ii. Real-time streaming content may include (but not be limited to) RealNetworks Real Media, Microsoft Windows Media, and Apple QuickTime.
    c) On-demand Streaming:
        i. The contractor shall host (i.e., provide storage) and deliver streams on demand or when requested by end-users (the CDNS shall encode the signal when sent in raw signal format by the content provider).

   ii. On-demand streaming content may include (but not be limited to) RealNetworks Real Media, Microsoft Windows Media, and Apple QuickTime.

2. Site Monitoring/ Origin Server Performance Measurements:
   a) The contractor shall perform continuous monitoring to ensure performance and quality of service. Measurements shall include:
      i. Availability
      ii. Latency
      iii. FTP Load
      iv. CPU Load
      v. Memory Usage
      vi. TLS Service Load
      vii. HTTP Port Service Load
      viii. HTTP Connections Queue Statistics
   b) The contractor shall provide statistics via a performance dashboard – a secure, Web-based portal accessible 24x7 by agency clients. The performance dashboard shall be consistent with commercial best practice.

C.2.5.4.2 Features

The following features are mandatory unless marked optional:

1. Failover Service: This service monitors single-location web sites (maintained by agencies or third parties under contract to agencies) and redirects traffic to a CDNS in the event of failure. This service shall ensure that end-users do not experience delays, site inaccessibility, or error messages.
2. (Optional) Redirection and Distribution Service (Global Load Balancing): When users type in a web site address or Universal Resource Locator (URL), they rely on Domain Name System (DNS) servers to direct them through the Internet and connect them to the specified Web server. Redirection and distribution services ensure that all Web requests are directed to the closest, most available cache server. Typically a set of surrogate servers is provisioned to cache content for the content provider's origin server, enabling requests to bypass congested areas. Redirection and Distribution Services may employ any proven technique(s) including, but not limited to:
   a) DNS Redirection
   b) URL Rewriting
   c) Layer-4 Switching
   d) Layer-7 Switching
   e) HTTP Redirection

C.2.5.4.3 Interfaces

The contractor shall provide the following UNIs:

1. For access via Internet: Hyper Text Transfer Protocol (HTTP).
2. For agency connectivity to the CDNS server: UNIs as defined in VPN Service (VPNS). See Section C.2.1.1 for details.

C.2.5.4.4 Performance Metrics

The contractor shall comply with AQL of KPIs for CDNS as defined in Section C.2.5.4.4.1 below.

C.2.5.4.4.1 Performance Metrics for CDNS

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability (CDNS network)	Routine	99.99 %	99.99 %	See Note 1
GOS (Time to refresh content)	Routine	5 minutes	≤ 5 minutes	
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. CDNS availability is calculated as a percentage of the total reporting interval time that the CDNS is operationally available to the agency. Availability is computed by the standard formula:

$$Av(CDNS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

C.2.6 Wireless Service

C.2.6.1 Service Description

C.2.6.1.1 Functional Definition

Wireless Service (MWS) is a wireless transmission service for mobile and fixed terminals. The contractor provides the wireless network.

The services and bandwidth provided depend on the characteristics of the terminals and the technology used in the contractor’s wireless network and service platforms.

Short Messaging Services (SMS), a feature of MWS, provides the capability to send and receive text messages. The text can comprise of any alphanumeric characters; each short message may be up to 160 characters in length.

Multimedia Messaging Service (MMS), a feature of MWS, provides the capability to send and receive multimedia, such as pictures, streaming video, sound, and graphics.

C.2.6.1.2 Standards

MWS shall comply with the following standards:

1. 2.5G [based on General Packet Radio Service (GPRS) or Code Division Multiple Access (CDMA-2000 – 1xRTT)]:
   a) ETSI GSM-MAP
   b) TIA IS-41
2. 3G [based on CDMA] ITU-RTT IMT-2000:
   a) European ETSI/GSM Wideband CDMA (WCDMA) (also known as Universal Mobile Telecommunications System (UMTS))
   b) US CDMA Development Group (CDG) CDMA-2000 Evolution Data Optimized (EV-DO)
3. 4G [based on 3GPP Long Term Evolution (LTE)]:
   a) ETSI TR25.913
4. 5G
   a) IMT-2020 Standard
   b) 3GPP ITU-R M [IMT-2020 SPECS]
   c) Future Generation of cellular radios and other SRE
5. Wireless Application Protocol (WAP):
   a) WAP Forum (Wireless Application Protocol (WAP 1.1 and 2.0) via WAP Gateway)
   b) IP Mobility Support, IETF RFC 2002
6. 3G Security:
   a) 3GPP TS 21.133
   b) NIST FIPS Publication 140-2/3
7. Short Messaging Service (SMS)
   a) 3GPP TS 03.40
   b) GSM 03.41

8. Multimedia Messaging Service (MMS):
   a) 3GPP TS 23.140
   b) Open Mobile Alliance
9. The contractor shall comply with new versions, amendments, and modifications made to the above-listed documents/standards including beyond 5G.

C.2.6.1.3 Connectivity

MWS shall connect to and interoperate with the following:

1. The Public Switched Telephone Network (PSTN) and the worldwide dialing plan per ITU Recommendation E.164
2. Originate and terminate calls to users of commercial satellite-based services
3. The Internet
4. Agency mobile terminals, such as, but not limited to cellular phones, smartphones, wireless-enabled tablets, Notebook and Laptop PCs, and PDAs

C.2.6.1.4 Technical Capabilities

The following MWS capabilities are mandatory unless marked optional:

1. MWS shall have the capability to originate and receive voice calls from mobile phones, fixed wireline networks, and satellite-based networks.
2. The contractor shall provide mobile devices (smartphones, tablets, and cellular phones) as required (see Section C.2.10 Service Related Equipment) supporting the following capabilities:
   a) Cellular Phones:
      i. Built-in available features
      ii. Wireless broadband devices (e.g., mobile Wi-Fi hotspots, MiFi - wireless router that acts as a mobile Wi-Fi hotspot)
      iii. Secure voice communications with FIPS-compliant encryption (as available)
      iv. AC Charger
      v. (Optional) Headset/hands-free device
      vi. (Optional) Protective case
      vii. (Optional) Car Charger
      viii. (Optional) Spare or extra battery
      ix. (Optional) Holster
   b) Smartphones and Tablets:
      i. Built-in available features
      ii. Short Messaging Services (SMS) (i.e., text messaging)

iii. Multimedia Messaging Services (MMS)
iv. Email
v. Web browser
vi. Personal Information Management (PIM), including contact and calendar information and documents/notes
vii. Ability to sync with leading email, contact/address, and calendar platforms
viii. Vibrate alert to emails and text messages
ix. Ring alert to emails and text messages
x. Ability to transfer photos/pictures directly to computer
xi. Remote kill (as available)
xii. Remote wipe (as available)
xiii. Ability to disable audio, video, and all recording functionality (as available)
xiv. Transmit and receive data (e.g., run an agency specific app, access the Internet) while conducting a voice session (as available)
xv. AC Charger
xvi. (Optional) Headset/hands-free device
xvii. (Optional) Protective case
xviii. (Optional) Car Charger
xix. (Optional) Spare or extra battery
xx. (Optional) Holster

3. The contractor shall offer the following MWS plans and plan aspects for GFP and user-owned devices.

   a) Voice Service Plans shall include voice calling and text messaging (SMS).

   b) Data Add-On Service Plans shall include data added to voice service plans. Data may include email, Internet access, video, Multimedia Messaging Service (MMS), and other data.

   c) Data only Service Plans shall include emails, Internet access, video, MMS, and other data transport not combined with voice service plans.

   d) (Optional) Machine-to-machine (M2M) – M2M and telemetry products shall provide wireless connectivity to machines, vehicles, or assets

   e) Mobility applications for mobile device management (see Section C.2.8.6 Managed Mobility Service).

   f) Domestic Mobile Roaming is included in all Domestic calling plans at no additional charge to the government and will include voice calls, messaging, multimedia, and data.

   g) (Optional) Non-Domestic Mobile Roaming Plans shall cover voice calls, messaging, multimedia, and data.

h) Pooling of domestic data. Pooling of domestic data (gigabytes) within the same billing account at a level specified by the ordering entity (e.g., an entire agency or multiple sub-bureaus within an agency).

4. The contractor shall comply with Wireless Enhanced 911 (E911) Rules including Phases I and II as stipulated by the Federal Communications Commission. Refer to http://www.fcc.gov/911/enhanced/.
5. No Additional Charge Items: There shall not be any additional charges for the following:
    a. International charges if the transmission originates and terminates at domestic locations, regardless of whether international roaming is activated (as available).
    b. Third-party direct billing
    c. In-network mobile-to-mobile minutes
    d. Contractor owned Wireless Local Area Network (WLAN) (e.g., Wi-Fi) usage. The use of non-domestic/international Wi-Fi calling will generate additional charges per the associated voice plan of the line.
    e. Activation/establishment or service restoration including internal/external porting of telephone numbers, telephone number changes, and/or to change or activate/deactivate service features
    f. Termination
6. (Optional) Emergency service plans will be offered for devices that typically are not used except during emergencies.
7. (Optional) SRE capable of supporting multiple SIM cards or one SIM card and one ESIM.
8. (Optional) SCIF friendly mode feature SRE will, with a press of a single button or key, and as verified with a SCIF-mode indicator LED or icon, enable SCIF friendly mode. The transmit and receive functions can be ‘turned off’ to enable use in a secure space when policy allows. In “SCIF Friendly” mode, all transmitters, receivers, microphones, speakers, transducers, GPS, and recording capabilities in the device are shutdown while still allowing the user to access the PDA functions like appointment/schedule calendars, contacts, checking previously downloaded email, and viewing documents. SCIF Friendly mode smartphones shall not be equipped with a camera.
9. (Optional) Software licenses and support services that enable maintenance, encryption, and security compliance services (including FIPS 140-2/3 compliance) for use with the provided SRE.
10. (Optional) Cellular connectivity to a wide area network (WAN)
11. SRE Replacement/Refresh

   a. Warranty: The Contractor shall state its warranty policy, which shall include a minimum of a 30 day SRE return policy following receipt during which period the user may return the SRE and obtain an equivalent replacement without penalty.
   b. Device Refresh: The Contractor shall offer refresh SRE after no more than 20 months of activation. An Ordering Entity may refresh SRE with the device options and obligations of a new activation. For SRE activated less than 20 months, the Contractor shall publish its method for determining the refresh price.

12. Support Interface
    a. The interface shall support the following requests/commands being sent to the Contractor. The Contractor shall state the target and maximum amount of time that the below commands shall take.
       i. Activate and deactivate devices
       ii. Reset voicemail passwords
       iii. Suspend/resume a line of service
       iv. (Optional) Kill a device
       v. (Optional) Wipe a device
       vi. Submit trouble tickets
    b. The Contractor shall provide acknowledgements of all requests/command completions, which shall be sent to the agency designated point of contact. Trouble ticket updates shall be updated as the agency requires.
13. Usage Data and Notifications. The Contractor shall provide usage data information and excessive usage notifications. This includes a summary of how much data has been used within an ongoing billing period to potentially provide an agency with an advanced indication that it may run over its allocated pooling GBs.
14. The Government will own all user privacy data, including the name of the individual using the service, all contact information, usage information and inventory data. The Government will also own all content sent to the Government including emails, text messages, data, and voicemails.

C.2.6.2 Features

The following features are mandatory unless marked optional:

1. Wireless Priority Services (WPS). WPS allows authorized National Security and Emergency Preparedness (NS/EP) personnel to gain access to the next available wireless radio channel in order to initiate calls during an emergency when channels may be congested. WPS is invoked by dialing *272 prior to the destination number on wireless terminals that have subscribed to WPS. Refer to http:/wps.ncs.gov/. Also see Section G.11.4.2, for NS/EP requirements.

2. Directory Assistance with Call Completion. This feature allows the user to obtain at least two look-up phone numbers and connect to one of them.
3. Domestic to Non-Domestic Calling. This feature allows a user to make non-domestic calls.
4. (Optional) International Mobile Roaming. This feature allows a user to roam internationally with wireless Internet connectivity and communications capability. International long distance and international roaming prices shall be “add-ons” to existing voice or data pricing.
5. Personal Hotspot. This feature enables a wireless device to be used as a hotspot to connect another device to the Internet or to a private network.
6. Indoor cellular system (Femtocells and Microcells) installation to allow and/or improve indoor wireless operation.
7. (Optional) Push to Talk with Group Talk enables users to connect directly with other users by pressing a button on their wireless terminals. The service shall indicate via an icon on the handset whether a user on their calling list is available. Business colleagues or work teams shall be able to set up and manage group calling lists. This capability shall support groups of up to 10 participants. Users can create up to 50 group lists and store 100 individual contacts.

C.2.6.3 Interfaces

The contractor shall support the following interfaces for the provisioning of MWS at the SDP, as defined in Section C.2.6.3.1.

C.2.6.3.1 Wireless Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
1	GSM and IS-136 TDMA	Up to 116 Kbps	1. Transparent 2. IP v4 3. IP v6
2	CDMA 1xRTT	Up to 144 Kbps	1. Transparent 2. IP v4 3. IP v6
3	3G WCDMA	Up to 384 Kbps	1. Transparent 2. IP v4 3. IP v6
4	CDMA EVDO	Up to 500 Kbps	1. Transparent 2. IP v4 3. IP v6
5	WCDMA-HSDPA [Optional]	Up to 14.4 Mbps	1. Transparent 2. IP v4 3. IP v6

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Protocol Type
6	4G LTE	Up to 100 Mbps (maximum 300 Mbps)	1. Transparent 2. IP v4 3. IP v6
7	5G and future evolutions	Up to 20 Gbps (Depending on configuration)	1. Transparent 2. IP v4 3. IP v6

C.2.6.4 Performance Metrics

The contractor shall comply with AQL of KPIs for MWS as defined in Section C.2.6.4.1 below.

C.2.6.4.1 Performance Metrics for Wireless Service

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Notes 1 and 2
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. MWS availability is calculated based on availability of access to the contractor's network from the contractor's cell site.
2. Radio access network performance is likely to vary depending on location (e.g., urban, suburban, or rural), as well as the technical specifications and capabilities of the deployed infrastructure, such as the radio access equipment.

C.2.7 Commercial Satellite Communications Service

C.2.7.1 Service Description

C.2.7.1.1 Functional Definition

The contractor shall provide mobile or fixed commercial satellite communications (COMSATCOM) services to include, but not be limited to: satellite bandwidth, satellite service plans, contractor provided earth terminals, radio frequency equipment, satellite phones, interfaces and support services. Specific services will be identified in TOs.

COMSATCOM shall be provided in any commercially available communications satellite frequency band to include, but not limited to, S-, C-, L-, X-, Ku-, Ka- and UHF bands.

Commercial Mobile Satellite Service (CMSS) delivers voice, data and Internet services to land-based, maritime, or aeronautical users using one- or two-way communications via satellite. The service provides an end-to-end connection between CMSS users, or between CMSS and wireline and wireless users via the contractor's network and gateway(s).

Commercial Fixed Satellite Service (CFSS) provides satellite capacity that can be used to deliver communications and applications at a customer-specified throughput between two or more specified end points. This service can be used for applications such as distance learning, continuity of operations, broadcast video and associated audio, including encrypted communications.

C.2.7.1.2 Standards

This section addresses CFSS standards. The air interface for a government-owned or -controlled earth terminal shall be at the terminal antenna. Government-owned terminals will provide the capability of handling multiple CFSS carriers. The government terminals shall be considered as conforming to the mandatory requirements of Military Standard (MIL-STD)-188-164 with associated modems conforming to MIL-STD-188-165.

Satellite services are required to be provisioned by the contractor in accordance with the following priority:

1. Utilization of satellites compliant with DODI 8581.01.
2. Utilization of other available satellites when DODI 8581.01 compliant satellites are not available shall be contingent upon the cognizant CO and COR accepting the associated risk.

For CMSS, the contractor shall support the following standards:

1. North American Numbering Plan (NANP)
2. ITU-TSS World Numbering Plan (Standard: ITU-TSS E-164)
3. IETF RFCs for IPv4/v6
4. Proprietary air-link interface standards based on mobile satellite systems, such as the Inmarsat Broadband Global Area Network (BGAN) and the Iridium satellite constellation

The contractor shall provide domestic and non-domestic satellite services when required in the TO.

C.2.7.1.3 Technical Capability

The contractor shall provide space segments to meet the requirements specified in the TO and, at a minimum, the performance requirements specified in Section C.2.7.3. For dedicated capacity requirements, the contractor shall provide satellite bandwidth on a non-preemptable basis unless otherwise specified in the TO. That is, the bandwidth shall not be preempted for any reason, and shall be replaced in the event of failure.

The contractor shall provide contractor-operated and -maintained leased earth terminal services as specified in individual TOs. Earth terminals provided by the contractor shall be certified as acceptable for service by the satellite system operator of the specific system on which the earth terminal is to be used.

The contractor shall provide CFSS Satellite Internet Service (SIS). The SIS shall provide Internet access as well as domestic and international voice service.

For CMSS, the contractor shall support Internet access, voice calling, SMS texting, fax, streaming services, and M2M.

C.2.7.2 Features

The following CFSS features are mandatory for delivery of COMSATCOM:

1. Capacity: The contractor shall be able to provide scalable capacity in any available COMSATCOM frequency band in support of US Government COMSATCOM requirements, subject to the availability of satellite resources.
2. Coverage: The contractor shall be able to provide coverage anywhere worldwide in any available COMSATCOM frequency band, including, but not limited to, L-, S-, C-, X-, Ku-, extended Ku-, Ka-, and UHF. Specific pre-defined coverage may be negotiated and defined in the TO. This requirement is subject to the availability of satellite resources.
3. Network Monitoring (Net OPS): The contractor shall have the capability to electronically collect and deliver near real-time monitoring, fault/incident/outage reporting, and information access to ensure effective and efficient operations, performance, and availability, consistent with commercial practices. The Net OPS information will be provided on a frequency (example: every 6 hours, daily) and format (example: SNMP, XML) consistent with the contractor’s standard management practices, to a location/entity/electronic interface as defined in a requirement by the OCO. Specific reporting requirements will be defined by the OCO.
4. EMI/RFI Identification, Characterization, and Geo-location: The contractor shall have the capability to collect and electronically report in near real-time Electro-

Magnetic Interference (EMI) / Radio Frequency Interference (RFI) identification, characterization, and geo-location, including the ability to identify and characterize sub-carrier EMI/RFI being transmitted underneath an authorized carrier, and the ability to geo-locate the source of any and all EMI/RFI. The contractor shall establish and use with the OCO a mutually agreed-upon media and voice communications capability capable of protecting CUI data.

5. Interoperability (Net Ready): COMSATCOM services shall be consistent with commercial standards and practices. Services shall have the capability to access and/or interoperate with government or other commercial teleports/gateways and provide enterprise service access to or among networks or enclaves.
6. Information Assurance: The contractor shall meet the following standards as applicable:
   a) The Committee on National Security Systems Policy (CNSSP) 12, “National Information Assurance Policy for Space Systems used to Support National Security Missions,” or
   b) DODI 8581.1, “Information Assurance (IA) Policy for Space Systems Used by the Department of Defense.”

The contractor shall demonstrate the ability to comply with FISMA as implemented by Federal Information Processing Standards Publication 200 (FIPS 200), “Minimum Security Requirements for Federal Information and Information Systems.” At a minimum, all services shall meet the requirements assigned against a low-impact information system (per FIPS 200) that is described in the current revision of NIST SP 800-53, “Security Controls for Federal Information Systems and Organizations.”

The contractor’s information assurance boundary is defined as where the contractor’s services connect to the user terminals/equipment (i.e., includes satellite command encryption (ground and space); systems used in the Satellite Operations Centers (SOCs), Network Operations Centers (NOCs) and teleport; and terrestrial infrastructure required for service delivery).

For CMSS, the contractor shall provide satellite phones/terminals (dual-mode (satellite/GSM) and tri-mode (satellite/CDMA/AMPS)) and encrypted transmission.

C.2.7.3 Performance Metrics

The contractor shall provide domestic and non-domestic CFSS and CMSS as specified in the table below.

Satellite Performance Requirement (KPI)	Performance Specification (Threshold/AQL)
Availability (for both CFSS and CMSS)	≥ 99.5%
For CFSS:	
Error Free Seconds (EFS)	> 0.965
Severely Errored Seconds (SES)	≤ 0.0003
Degraded Minutes (DM)	≤ 0.02
Mean Time to Loss of BCI (MTTLBCI)	≥ 24 hours
Delay (One Way)	The lesser of 450 ms or (260 + 0.01 x D ms) (See Note 2)

Notes:

1. CFSS and CMSS availability is calculated as a percentage of the total reporting interval time that they are operationally available to the agency. Availability is computed by the standard formula:

$$Av(CFSS \ \& \ CMSS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. "D" is the SDP-to-SDP transmission distance, measured via the shortest great circle, in kilometers.

C.2.8 Managed Service

Managed service is the practice of outsourcing day-to-day customer management responsibilities and functions to the service provider as a strategic method for improving operations and cutting expenses. The managed service provider is accountable for the functionality and performance of the managed service.

Managed services provide the delivery and management of network-based services, applications, solutions, labor and equipment needed to the enterprises. The managed service includes a) service planning and solution engineering, b) solution implementation (including labor and equipment), c) service provisioning, d) end-to-end service management (including LAN routers and WAN), and e) service assurance (performance metrics and SLA management).

C.2.8.1 Managed Network Service

C.2.8.1.1 Service Description

Managed Network Service (MNS) enables an agency to obtain design and engineering, implementation, management, and maintenance services for agency networks. MNS provides the necessary technical and operational capabilities that ensure the availability and reliability of agencies' increasingly complex networks.

When MNS is used with a single EIS service (e.g., VPNS) or a group of EIS services (e.g., VPNS, Ethernet, voice service, and cloud IaaS) requested in a TO, those services will have the functionalities of a managed service (i.e., Managed VPNS, Managed Ethernet, Managed voice service, and Managed Cloud IaaS).

The contractor shall use the appropriate labor and equipment as defined in Section C.2.10 Service Related Equipment and Section C.2.11 Service Related Labor in the TO.

C.2.8.1.1.1 Functional Definition

Under the MNS offering, the contractor provides overall management of an agency's network infrastructure, including real-time proactive network monitoring, troubleshooting and service restoration. The contractor is the agency's single point of accountability for all networks managed under this service, including operations, maintenance, and administration activities.

C.2.8.1.1.2 Standards

MNS shall comply with the following standards:

1. All appropriate standards for any underlying EIS access and transport services
2. The specific standards and requirements identified in the TO

C.2.8.1.1.3 Connectivity

MNS shall work with underlying EIS offerings such as VPNS, PLS and other services as needed, to ensure seamless connectivity to agency networking environments.

C.2.8.1.1.4 Technical Capabilities

The following MNS capabilities shall be provided by the contractor.

C.2.8.1.1.4.1 Design and Engineering Services

The contractor shall provide design and engineering services that include, but are not limited to:

1. Identify hardware and firmware (e.g., routers, switches, and other SRE), related software, and SRL required by the agency to deliver the EIS services.
2. Identify network components and determine protocols, redundancy, traffic filtering, and traffic prioritization requirements. Recommend the appropriate performance levels and network capacities as required.
3. Provide complete project management for design, engineering, implementation, installation, access coordination, provisioning, equipment configuration, hardware testing, and service activation. Coordinate installation activities with the agency to minimize the impact on the current networking environment.

C.2.8.1.1.4.2 Implementation, Management and Maintenance

1. The contractor shall develop, implement, and manage comprehensive solutions using the EIS services to meet agency-specific requirements. The solutions shall include, but are not limited to:
   a) Access solutions that use a combination of different services (e.g., wireline and wireless access services) for specific agency locations, to meet agency performance metrics for availability and disaster recovery.
   b) Transport solutions that distribute traffic over multiple contractor backbone networks to provide redundancy and carrier diversity, and vary the traffic allocation dynamically based on agency performance requirements.
   c) Customer premises solutions that provide agency-specific interfaces, software, and equipment to meet agency requirements.
   d) Security solutions as required by the agency.
2. The contractor shall supply and manage the hardware, firmware and related software required by the agency. Components include but are not limited to routers and switches, encryption devices, CSUs/DSUs, hubs, adapters, and modems.
3. The contractor shall provide tools to:
   a) Monitor performance of agency-specific networks including transport services, access circuits, and government edge routers
   b) Provide real-time visibility of transport and access services performance
4. The contractor shall:
   a) Manage the network in real-time on a 24x7 basis
   b) Support remote management capabilities from the operations center defined in the TO
   c) Proactively monitor utilization and performance, probing in intervals of no more than fifteen minutes to ensure proper equipment/network operations

   d) Assess and report access and transport services performance and SLAs
   e) Assess and report on agency-specific network capacity and performance
   f) Address agency-specific network capacity and performance issues

5. The contractor shall permit SNMP read-access data feeds that provide the agency with managed equipment information, as applicable.
6. The contractor shall manage network configuration. Activities shall include but are not limited to the following:
   a) Adding a protocol
   b) Adding, moving or removing Customer Premises Equipment (CPE)
   c) Changing addressing, filtering, and traffic prioritization schemes
   d) Optimizing network routes
   e) Updating equipment software and/or configuration, including but not limited to firewall and VPN security devices
   f) Upgrading or downgrading bandwidth
   g) Implementing configuration changes for all agency-specific devices
   h) Maintaining a configuration database for all agency-specific devices
   i) Auditing government router configurations
7. The contractor shall provide IP Address Management as applicable. The contractor shall submit agency-completed American Registry for Internet Numbers (ARIN) justification requests for specified IP allocations in order to support the service offered.
8. The contractor shall monitor and control access to equipment under its control including limiting access to authorized personnel, and implementing passwords and user permissions as directed and approved by the agency.
9. The contractor shall regularly perform off-site equipment configuration backups, in order to ensure the availability of recent configuration data for restoration purposes. The contractor shall provide the agency with secure access to backup logs as needed.
10. The contractor shall perform necessary hardware and software upgrades, updates, patch deployments and bug fixes as soon as they become available. The contractor shall implement updates in coordination and mutual agreement with the agency and test new releases to resolve any security concerns, ensure compatibility with the agency environment, minimize service disruptions, and maintain equipment functionality.
11. The contractor shall provide preventative and corrective maintenance on agency-specific devices.

12. The contractor shall proactively detect problems, respond to alerts and promptly report situations that adversely affect throughput to the agency. The contractor shall provide notification of alarms, network troubles and service interruptions via email, telephone, or as specified in the TO. The contractor shall:
    a) Monitor agency-specific network availability and quality of service (e.g., network delays, packet loss)
    b) Monitor access circuit availability and QoS
    c) Monitor the government's edge router availability and performance
    d) Monitor transport service availability at the government's network equipment
    e) Monitor agency-specific network performance from government network equipment to government network equipment
    f) Monitor transport service availability up to the government's network equipment
    g) Monitor transport service performance from government network equipment to government network equipment
    h) Provide, monitor and manage circuits for out-of-band government network equipment management
    i) Open/close trouble ticket in agency's trouble ticketing system
    j) Open/close trouble ticket in contractor's trouble ticketing system
    k) Troubleshoot access and transport services faults and coordinate faults resolution/repairs
    l) Troubleshoot government network equipment faults and coordinate resolution/repairs.
    m) Troubleshoot agency-specific network faults
    n) Notify agency-specific network users of faults and maintenance via agency alerts
    o) Answer NOC Help Desk phones and provide Tier-1 support to agency-specific network users
    p) Provide Tier-1/Tier-2/Tier-3 support to agency NOC for contractor access and transport services
    q) Provide Tier-1/Tier-2/Tier-3 support to agency NOC for the components of the Agency's network that are managed by the contrtactor.
13. The contractor shall provide the agency with real or near-time access to the following:
    a) Installation schedule detailing the progress of activities such as the implementation of equipment, access and transport circuits, and ports, as applicable. This allows agencies to track the provisioning process through

completion at any time. Near real-time access to the installation schedule is acceptable.

b) Network statistics and performance information including equipment data availability, throughput and delay statistics, CoS settings, and application-level performance information.

c) Trouble reporting and ticket tracking tools

d) Security logs

14. The contractor shall provide inventory tracking tool(s) to maintain and track all agency circuit, transport service and equipment inventory information.

15. The contractor shall provide the agency with secure access to current and historical information which includes, but is not limited to, the following:

    a) Bandwidth and service quality information
    b) Burst analysis identifying under or over utilization instances
    c) Data errors
    d) Delay, reliability and data delivery summaries
    e) End-to-end network views
    f) Exception analysis
    g) Link, port and device utilization
    h) Network statistics
    i) Protocol usage
    j) CPU utilization
    k) Traffic, port and protocol views

C.2.8.1.2 Features

The contractor shall provide the following features:

1. GFP and SRE Maintenance. The contractor shall maintain and repair GFP and SRE.

2. Agency-Specific Network Operations Center (NOC) and Security Operations Center (SOC). The contractor shall provide agency-specific help desk services and shared or dedicated NOCs and SOCs to meet agency requirements.

3. Network Testing. The contractor shall support agency-specific development services which address the agency‘s potential need to test equipment, software and applications on the contractor’s network prior to purchase and deployment. This shall cover voice, data, and video technologies that include but are not limited to IP VPN and voice services. Testing shall be performed at the agency’s discretion and structured in collaboration with the contractor.

4. Traffic Aggregation Service (DHS Only). The contractor shall establish and maintain secure facilities ("DHS EINSTEIN Enclaves") where DHS-furnished equipment can be deployed, provide network connectivity from the DHS EINSTEIN Enclave to the DHS data centers, and route all traffic subject to National Policy requirements described in Section C.1.8.8 through (i.e., deliver to and receive from) a DHS EINSTEIN Enclave for processing by the latest generation of EINSTEIN capabilities. Once traffic is received at the EINSTEIN Enclave and processed, it is sent back to the contractor for delivery to its destination. The contractor shall assume responsibility for maintaining and repairing the traffic aggregation service, including associated commercial security services and all communications links, and shall provide engineering support to integrate the DHS GFP sensor equipment, data center and communications infrastructure into the contractor's services. The contractor shall assist DHS in the maintenance and repair of the sensor system to the extent of receiving phone calls or emails requesting "Smart-Hands" service of DHS-supplied equipment.

C.2.8.1.3 Interfaces

MNS shall support the UNIs for all underlying EIS access and transport services.

C.2.8.1.4 Performance Metrics

The MNS performance levels will be specified in the TO.

C.2.8.2 Web Conferencing Service

C.2.8.2.1 Service Description

Web Conferencing Service (WCS) enhances traditional conferencing by offering the capability to meet, present, and interact with information via a web browser.

C.2.8.2.1.1 Functional Definition

WCS allows agencies to share information, documents, or applications interactively via the Internet and the agency's Intranet.

C.2.8.2.1.2 Standards

WCS shall comply with the following standards:

1. Hyper Text Transfer Protocol (HTTP)
2. Hyper Text Transfer Protocol Secure (HTTPS)
3. (Optional) IETF RFC 3261 for Session Initiation Protocol (SIP)
4. ITU-T T.120 Series of Data Protocols for Multimedia conferencing
5. Transport Layer Security (TLS) Encryption

6. Transmission Control Protocol/Internet Protocol (TCP/IP) Suite

The contractor shall comply with new versions, amendments, and modifications made to the standards listed above.

C.2.8.2.1.3 Connectivity

WCS shall connect to and interoperate with:

1. Agency Intranet
2. Internet

WCS shall be accessible via a Universal Resource Locator (URL) address.

C.2.8.2.1.4 Technical Capabilities

The following WCS capabilities are mandatory unless marked optional:

1. The contractor shall provide a capability that enables participants to collaborate. This shall include real-time document sharing, file transfer capability and electronic whiteboards in a private and secure WCS session.
2. The contractor shall provide the following capabilities:
    a) Authentication and password protection
    b) Customized greeting (or message) screen
    c) Online Help
    d) Support for point-to-point and multi-point Web conferences
3. The WCS shall interoperate with the Internet and ordering agencies' IP network(s).
4. The WCS shall be compatible with available Web browser software packages. Appropriate plug-ins shall be provided in order to deliver WCS to the user.
5. The contractor shall provide a means by which users can test and verify that their web browser and desktop software are compatible with WCS service prior to the scheduled conference. If required, the contractor shall provide the appropriate plug-ins to deliver WCS to the users. The browser plug-in shall be limited to utilities required for the user to play back, participate in, or lead a web conference session. This can include plug-ins that enable users to play back recorded conferences from their web browser, develop WCS presentation slides within existing agency-owned software applications (i.e. Microsoft PowerPoint) or view WCS from mobile devices.
6. The WCS shall support dynamic content (i.e., the ability to use Audio Visual Interleave (AVI's) files, flash, animated gif, and dynamic html pages).
7. The WCS shall be available on demand or via a scheduled reservation.
8. The contractor shall provide a reservation system with the ability for authorized WCS users to schedule or cancel web conferences at least one year in advance.

Scheduling may be by time and day of the week, either as a single event or recurring event on a daily, weekly, monthly, or on another periodic basis.

9. The contractor shall provide an email notification with a meeting invitation and RSVP to WCS participants.
10. The contractor shall provide the capability to extend the scheduled conference time upon request from the ordering agency and to add participants.
11. The WCS shall be secure and provide authentication and encryption capabilities to identify and authenticate users before providing access.
12. The WCS shall be accessible via a Universal Resource Locator (URL) address with a login and password for valid participants.
13. The contractor shall provide passwords for both conference leaders and participants.
14. The WCS shall provide the capacity to support at least 1,000 simultaneous participants in an individual Web conference.
15. The WCS shall have the capability to traverse and successfully interoperate with agency firewalls and security layers. The contractor shall verify with the agency that the agency firewall is compatible with this service.
16. The contractor shall provide the capability for users to request operator assistance to immediately resolve WCS service issues or problems.
17. The WCS shall provide annotation (i.e., the ability to emphasize a specific area of a presentation slide with a marker or pointer tool).
18. The WCS shall provide a participant list (i.e., the ability to view the names of other participants attending the WCS presentation).
19. The contractor shall support group web surfing (i.e., the ability for the conference leader to guide and navigate WCS participants to a web page).
20. The contractor shall support file transfer (i.e., the ability to upload a file that a WCS participant can download within the meeting or event). The file transfer can be sent to all participants or selected participants. The receiving participant shall have the option to accept or reject the file transfer.
21. The contractor shall support multiple presenters on a WCS meeting or event.
22. The contractor shall support video webcasts to no fewer than 3,500 participants.
23. The contractor shall provide polling and voting capability. This allows the conference leader to pose questions and receive feedback from participants during a presentation with a variety of different answer sets (multiple choices, open ended, yes/no) on demand. The participant shall have the capability to signal the conference leader when they have a question.
24. WCS polling/voting feedback shall be available instantly for the WCS conference leader and, if requested, via a polling/voting results report.

25. (Optional) The contractor shall provide a meeting lobby to allow conference leaders to admit participants to the meeting, as well as the ability for conference leaders to lock and unlock access to the meeting. When the meeting is "locked," no additional participants are allowed to join the active conference.
26. The contractor shall provide the capability for conference leaders to print the presentation used during the conference or save it to a local file. Participants shall have the same capability if permitted by the conference leader.
27. WCS shall support text chat, which enables real-time text communications between WCS conference participants. This shall include support for a public text chat for all participants with the conference leader, and private chats between selected participants.
28. The contractor shall provide the capability to present a survey to all or a random percentage of participants to gather feedback and/or capture customer satisfaction data.

C.2.8.2.2 Features

The following WCS features are mandatory unless marked optional:

1. Streaming Audio: The contractor shall provide the ability to deliver one-way audio over the Internet during a WCS session. The streaming audio shall be synchronized with any data portions of the Web conference.
2. Streaming Video: The contractor shall provide the ability to deliver one-way video over the Internet during a WCS session. The streaming video shall be synchronized with any data portions of the Web conference.
3. Web Based Presentation Replay: The contractor shall provide the capability to replay (or play back) Web-based presentations. The replay shall be available for a minimum of 90 days after the initial conference. The contractor shall offer the agency an option for extending the conference replay, in 30-day increments, for a period of 1 year.

C.2.8.2.3 Interfaces

Not applicable – WCS is a browser based service.

C.2.8.2.4 Performance Metrics

The performance levels and AQL of KPIs for WCS in Section C.2.8.2.4.1 are mandatory unless marked optional.

C.2.8.2.4.1 Web Conferencing Service Performance Metrics

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability	Routine	99.9%	≥ 99.9%	See Note 1
Time To Restore	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Availability is measured and calculated as a percentage of the total reporting interval time that WCS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

.

C.2.8.3 Unified Communications Service

C.2.8.3.1 Service Description

Unified Communications Service (UCS) integrates multiple methods of communication, (e.g., e-mail, faxing, instant messaging, voice and video calling, conferencing that identifies which participant is speaking, mobile communication, and desktop sharing) in order to allow users to connect, collaborate, and exchange information. This may include real-time and non-real-time, “one-to-one”, “one-to-many”, and “many-to-many” bi-directional communications between internal and external entities. UCS can be implemented as an application hosted by the contractor that supports multiple users over an IP network (agency- or contractor-provided), or as a premises-based, hosted, or hybrid solution.

UCS combines independently-run communications subsystems in order to streamline how agency users and customers communicate and collaborate regardless of location.

C.2.8.3.1.1 Functional Definition

UCS supports a common user interface for agency communications subsystems, such as voice subsystems (VoIP based/enabled) and applications, including unified messaging, instant messaging, presence, voice mail, integration with email where applicable, fax, and video/ audio/web conferencing, and allows users to access messages with any device, anywhere, and at any time.

C.2.8.3.1.2 Standards

UCS shall comply with the following standards:

1. All applicable IETF RFCs for IP-based voice, data, and video applications, such as VoIP (SIP), TCP/IP, mail (SMTP, POP3, IMAP4, LDAP), and RSVP for call admission.
2. Common telephony and network standards, including but not limited to:
   a) SIP/SDP for call setup and trunking
   b) SRTP and G.711/G.722/G.729/H.264/OPUS CODEC, IETF RFC 6716 CODEC
   c) DSCP and LLDP for network traffic prioritization and device provisioning
   d) TLS and MTLS for session security
   e) ICE/STUN/TURN for NAT traversal and media relay for clients outside the firewall
   f) XMPP/SIP/PIDF for IM/presence federation
3. The specific standards as identified in the TO.
4. All appropriate standards for any applicable underlying EIS access and transport services.

C.2.8.3.1.3 Connectivity

UCS shall connect to and interoperate with:

1. PSTN (SIP trunk gateway).
2. Agency communication subsystems (e.g., voice, email, conferencing (audio, web-based video), instant messaging, presence, collaboration portals), over an IP network (agency provided or contractor provided).

C.2.8.3.1.4 Technical Capabilities

The following UCS capabilities are mandatory unless marked optional:

1. The contractor shall support enabling UC capabilities via many devices, including desktop phones and mobile devices (smart phones, tablets, etc.), wireline and IP phones, soft clients, and video conferencing devices.
2. Unified Messaging (UM) shall provide:
   a) User access to and management of voice mail, e-mail and fax messages through the same inbox or interface.

b) Modular messaging with access to messages from phones and PCs via various interfaces, including browsers.

c) The UC Messaging Directory, which acts as a container for all the UM objects and their configuration settings, shall logically represent a telephony hardware device and a telephony dial plan for the enterprise to support a specific UM feature.

d) The UC Messaging Directory objects shall enable the integration of UM with existing telephony infrastructure. The following UM objects shall be supported:

i. Dial Plans
ii. Mailbox Policies
iii. IP Gateways
iv. Hunt Groups
v. Auto Attendants
vi. Servers
vii. Users

3. Mobile Integration shall:

a) Provide users with a single identity that lets them handle business calls via their desk and mobile phones.

b) Provide users the ability to have calls forwarded to any phone and to use a single number for making and receiving all calls.

c) Support handing off calls from cellular to Wi-Fi connections and vice versa on smart phones.

d) Enable users to initiate phone calls, retrieve voice mail and corporate directories, access instant messaging and participate in video conferencing.

e) Provide features that are accessible from mobile phones, laptops and tablets, provide access to corporate directories and visual voice mail, and feature seamless handoff between cellular and Wi-Fi calls.

f) Allow calls to or from mobile devices to take place anywhere and anytime as if they are going to / coming from the desk phone numbers.

4. The Unified User Interface shall provide:

a) The ability for users to access UC capabilities from a variety of devices in a variety of ways.

b) Features such as presence, instant messaging, integrated soft phones, voice conferencing, video calling and conferencing.

c) Voice activation that integrates seamlessly with other business communication systems.

d) Real-time communications – instant messaging, presence that identifies which participant is speaking, voice calls to video, voice calls to email.

e) Non-real time communications – email, text messaging, fax, voice mail.

f) Collaboration and data sharing – electronic bulletin boards, e-Calendar, Audio/Video/Web conferencing.

g) The ability for users to access messages from the following:

   i. IP phones
   ii. Mobile phones
   iii. (Optional) Web browsers
   iv. E-mail clients
   v. Desktop clients
   vi. PCs
   vii. Tablets

h) Instant messaging between two users or multiparty (up to an agency-defined number of participants).

i) The ability for users to display their presence status (e.g., “Available,” “Away,” “Do Not Disturb,” “Busy,” or Offline) to let others know their availability for communication.

j) Presence integration with agency collaboration applications, such as calendaring, that automatically updates presence when users are in a meeting.

k) Audio and video conversations between two users or multiparty (up to an agency-defined number of participants), using web cameras, speakers and microphones.

l) File Transfer capabilities to send files between users.

m) Scheduled and ad hoc web conferencing for conducting online presentations including audio, video, screen sharing, and a virtual whiteboard. PC-to-PC and multiparty data sharing capabilities including desktop sharing, application sharing, presentations, virtual whiteboard, annotations, and polling.

n) Contact Groups that allow users to organize their contacts.

o) (Optional) Enhanced access to instant messaging from within the agency's enterprise network or from the Internet, through a variety of devices and software, in a secured mode using encryption.

p) Agency-managed instant messaging administration (add/change/delete users).

q) Single sign-in capabilities through the agency’s Enterprise Active Directory (EAD) system.

r) Automated and/or staffed UCS-dedicated Service Desk available 24/7.

5. The contractor shall provide the following capabilities to support QoS, if UCS is provided over the contractor's IP network:
   a) Configuration Options for QoS
   b) Traffic Prioritization
   c) QoS Queuing Methods and Scheduling
6. (Optional) The UCS shall provide a premises-based WAN optimizer to collect only the changes from each site, if the compilation of the current status of all users being logged on is transmitted over the agency WAN.
7. The UCS shall support both IPv4 and IPv6 and be able to communicate over IPv4-only, IPv6-only, and/or dual-stack networks.
8. The UCS shall meet a minimum voice quality level that is equivalent to or better than a Mean Opinion Score (MOS) of 4.0 as specified in ITU-T specification P.800 series.
9. The contractor shall ensure that security practices and safeguards are provided to minimize susceptibility to security issues and prevent unauthorized access. This includes SIP-specific gateway security for SIP firewalls where applicable. The contractor shall also comply with agency-specific security policies, regulations and procedures.

C.2.8.3.2 Features

None.

C.2.8.3.3 Interfaces

The contractor shall support UCS to different devices. At a minimum, the following shall be supported:

1. IP phones
2. Mobile phones
3. Web browsers
4. E-mail clients
5. Desktop clients
6. PCs
7. Tablets

C.2.8.3.4 Performance Metrics

The UCS performance levels and AQL of KPIs in Section C.2.8.3.4.1 are mandatory unless marked optional.

C.2.8.3.4.1 UCS Performance Metrics

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Note:

1. Availability is measured and calculated as a percentage of the total reporting interval time that UCS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

C.2.8.4 Managed Trusted Internet Protocol Service

C.2.8.4.1 Service Description

The requirements for government department and agency cybersecurity are evolving to incorporate advanced methods of aggregating and segregating inbound and outbound Internet traffic, Intrusion Detection, Intrusion Prevention, anti-virus and other services as supported by evolving commercially provided cyber-protection capabilities. Existing requirements are stated in this Section and will be updated according to DHS reference standards and OMB instructions in place at the time the RFP is issued.

The Managed Trusted Internet Protocol Service (MTIPS) allows agencies to physically and logically connect to the public Internet or other external connections, as required by the agency, in compliance with the Office of Management and Budget's (OMB) Trusted Internet Connections (TIC) update (M-19-26), announced in September 2019 which defines MTIPS applicability to the Traditional TIC use case. MTIPS facilitates security of Internet connections in government networks and provides standard security services to all government users.

MTIPS is comprised of the network infrastructure to transport IP traffic between the agency Enterprise WAN and the TIC Portal; together they create an agency TIC Trusted

Domain (DMZ) for IP traffic. In today's environment, the agency perimeter boundary is dynamic and morphing to include virtual instances.

MTIPS enables the government to react more effectively to cyber security attacks thus reducing malicious penetrations and theft of critical data. Exchange of information through the TIC Portal is closely monitored by an integrated MTIPS Security Operations Center (SOC) to protect agency IP traffic.

The MTIPS provided transport shall serve as a "collection" network for TIC physical or virtual Portal connectivity insulating an agency's internal network from the Internet and other external networks.

The TIC Portal shall function as an OMB approved Multi-Service Trusted Internet Connection Access Provider (TICAP) capable of hosting multiple agencies and able to manage and correlate multiple independent traffic streams for each ordering agency. The TIC Portal shall provide physical and virtual security services to multiple government clients, but allow for specific controls based on agency coordination, when necessary.

Each contractor shall build at a minimum two (2) TIC Domestic Portals that maintain physical diversity from the TIC Portals to its servicing Internet Exchange Point. The contractor shall provide management staff at each TIC Portal.

The contractor shall provide virtual TIC capabilities upon request for agencies with resources hosted outside their physical boundaries.

C.2.8.4.1.1 Functional Definition

The MTIPS generic functional model consists of the following set of functions and sub functions:

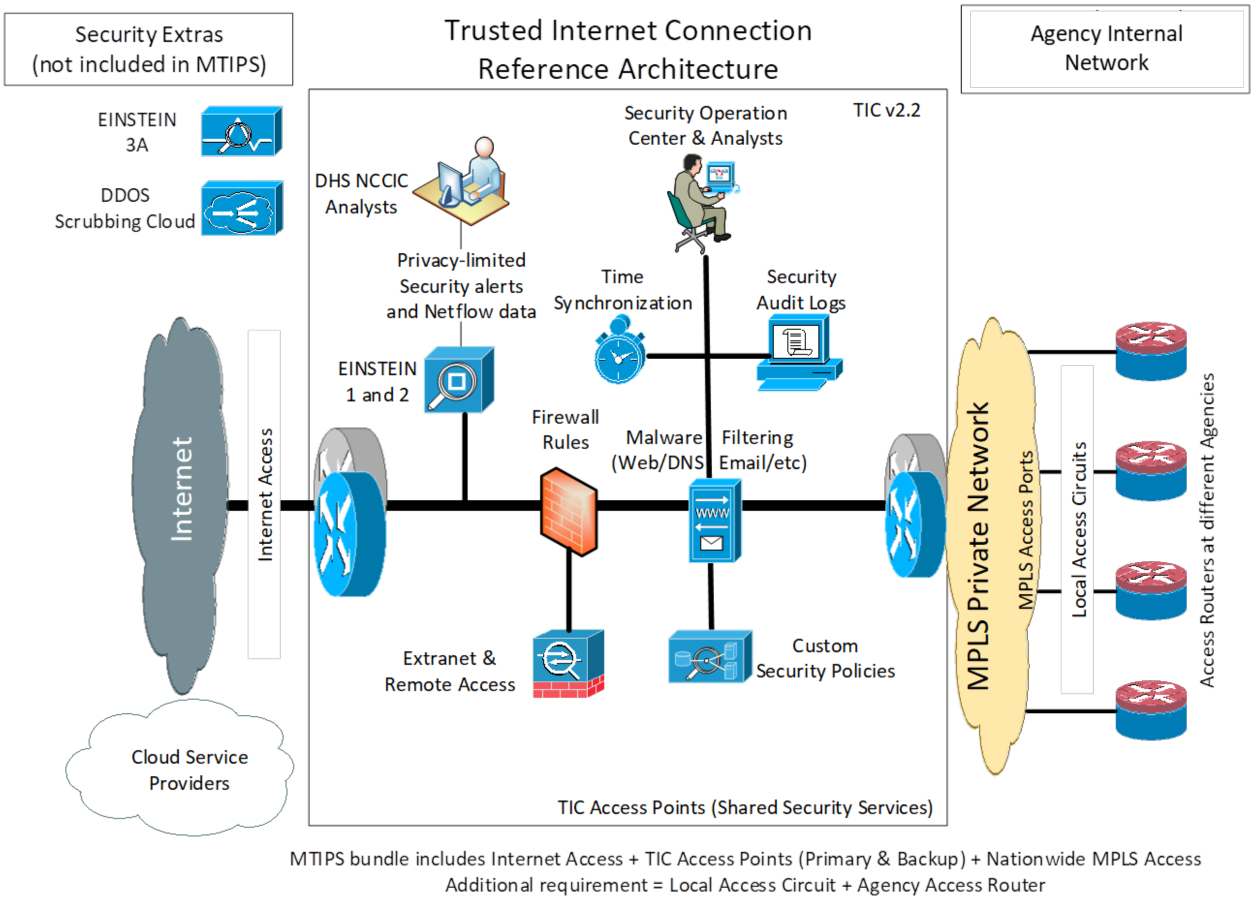
1. TIC Portal (TIC Access Points):
   a) Access to External Networks including the Internet
   b) Routing of traffic through EINSTEIN Enclave
   c) Security Operations Center (SOC)
2. Transport Collection and Distribution (MTIPS Transport)

The traffic collection and distribution supports the transport of government-only IP traffic between agency Enterprise network and TIC Portals utilizing the secure functionality of the SOC. The TIC Portal SOC monitoring and management systems shall be dedicated to the management and monitoring of the ordering agencies hosted by the contractor's portal and shall be isolated from commercial customers.

The MTIPS Context Architecture is defined in Figure C.2.8.4.1.1.1 below.

C.2.8.4.1.1.1 MTIPS Context Architecture

Figure 1*— The diagram below illustrates how data is collected from the agency WAN by the MTIPS transport network, and then directed to the TIC, which includes the Security Operations Center (SOC) and the Einstein Enclave.*



C.2.8.4.1.1.2 TIC Portal Security Operations Center Architecture

C.2.8.4.1.2 Standards

MTIPS shall comply with the following standards:

1. Current and future regulations, policies, requirements, standards, and guidelines for Federal U.S. Government technology and cyber security (e.g., the TIC Reference Architecture document) and within 90 days develop a plan for adoption. The contractor shall submit the plan to the CO within 90 days of issuance of new TIC capabilities or policy changes.

2. New document versions, amendments, and modifications. The most notable include minimum expectations for identified MTIPS-specified security services.

C.2.8.4.1.3 Connectivity

The MTIPS contractor shall connect and interoperate with:

1. The Public Internet
2. EINSTEIN Enclave
3. Reserved.
4. Rapid Response Loop from DHS to agency communications for the dissemination of threats/events to/from the agency
5. Other Agency IP Networks (External or Internal Connections)

C.2.8.4.1.4 Technical Capabilities

C.2.8.4.1.4.1 TIC Portal Capabilities

The following TIC Portal capabilities are mandatory, unless marked optional:

1. TIC Portal Access to External Networks including the Internet – To ensure that agencies are able to exchange traffic with the Internet and external networks at all times the TIC Portal shall comply with the following requirements when establishing interconnecting relationships:
   a) The TIC Portals shall connect to the Internet via Tier 1 Internet Service Providers (ISPs).
   b) The contractor shall budget enough interconnection bandwidth to accommodate increasing agency's demands.
   c) Alternate and diverse Routing – The contractor's TIC Portal shall provide multiple, physically diverse connectivity to interconnection points. The contractor shall consider single and multiple failure scenarios in the development of the technical architecture to demonstrate that KPIs and SLAs required in this document are met.
   d) Inter-carrier Routing Requirements – The ISPs and external networks converging to a portal shall run BGP (eBGP, BGP4, etc.) or one of the options for inter-AS connectivity as specified by the IETF.
   e) Support to Internet Protocol version 6 (IPv6) – The contractor shall also transport both IPv4 and IPv6 (i.e. dual-stack) between external connections, including the Internet, and agency's internal networks.
2. EINSTEIN Protection – The EINSTEIN Enclave includes the EINSTEIN devices providing customized threat mitigation, analytic, and network flow capabilities. The enclave in its entirety is provided by the government through separate means. At each TIC Portal the contractor shall meet applicable routing requirements in

Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.

3. TIC Portal Security Operations Center (SOC) – The TIC Portal SOC is the set of tools, appliances and processes that collect, reduce, normalize, correlate, fuse, and manage event data from a variety of devices that support the MTIPS operations. For the SOC, these devices include firewalls, Network Intrusion Detection Devices (NIDS), Host-based IDS (HIDS), and other platforms that may collect TIC Portal-relevant event data. The SOC tools also provide reports customized to agency's requirements but as a minimum shall support TIC Portal authorities / analysts by identifying security events of interest that may be negatively affecting the TIC Portal environment. The ordering agency's security authorities / analysts then will be empowered to react and trigger appropriate control mechanisms, thus creating a Rapid Response Loop. The primary goal of the SOC is to provide analysis/correlation and management structure to mitigate the threat presented by external attacks. Provide trained, qualified, and cleared staff (U.S. citizens) to support security functions 24x7. The SOC shall be staffed with at least two (2) people with appropriate credentials to manage technical aspects of the network attacks. The contractor shall comply with DHS-published TIC 2.0.
4. Reserved.
5. Content Filtering/Inspection of Encrypted Traffic with documented procedures.
6. Asymmetric Routing – The MTIPS portal stateful inspection devices shall correctly process traffic returning through asymmetric routes to a different MTIPS stateful inspection device; or shall document how return traffic is always forced to return to the originating MTIPS portal stateful inspection device.
7. Federal Video Relay Service (FedVRS) Support – The MTIPS portal shall support Federal Video Relay Service (FedVRS) for the Deaf (www.gsa.gov/fedrelay) network connections, including but not limited to devices implementing stateful packet filters.
8. E-Mail Forgery Protection – Domain-level sender forgery analysis equivalent to Domain Keys Identified Mail or Sender Policy Framework standards.
9. The contractor shall optionally support signing procedures for outgoing email messages to ensure that they have been digitally signed at the Domain Level (for example Domain Keys Identified Mail).
10. Domain Name System (DNS) and DNS Security Extensions (DNSSEC) – The MTIPS portals shall be equipped with resolving/recursive (also known as caching) name servers to properly filter DNS queries, and to perform validation of DNS Security Extensions (DNSSEC) signed domains for MTIPS subscribers. (Reference: NIST SP 800-81 Revision 1)

11. Uninterrupted Operations – The MTIPS portals shall be equipped for uninterrupted operations for at least 24 hours in the event of a power outage
12. Internet Protocol Version 6 (IPv6) – The contractor shall ensure that all TIC systems and components of the TIC portals support both IPv4 and IPv6 protocols in accordance with OMB Memorandum M-05-22, and the "IPv6 Transition Guidance" issued by the Federal CIO Council, Architecture and Infrastructure Committee."
13. Data Loss/Leak Prevention – The contractor shall support Data Loss (Leak) Prevention (DLP) program.

C.2.8.4.1.4.2 MTIPS Transport Collection and Distribution Capabilities

The following MTIPS Transport Collection and Distribution Capabilities are mandatory unless marked optional:

1. The contractor shall allow the agency's Internet bound traffic to reach the Internet via one of the two TIC Portals.
2. An agency Trusted Domain (DMZ) shall be created by the contractor to ensure that an agency's traffic is protected and physically isolated when transported to the portal and the public Internet. The DMZ includes the access portion of the service as well as the MTIPS transport. The contractor shall ensure that the traffic is not sniffable and ports cannot be spoofed.
3. Inter-agency traffic shall be routed through and inspected by the TIC Portal if the connection is classified as an external connection.

C.2.8.4.2 Features

1. Encrypted Traffic: The TIC Portal shall monitor, scan and filter the incoming and outgoing encrypted traffic traversing MTIPS (e.g., email, authorized / known bad mail, FTP and web traffic) which is proxied / non-proxied based on URL or IP address. The TIC portal shall analyze all encrypted traffic for suspicious patterns that might indicate malicious activity and shall keep logs of at least the source, destination and size of the encrypted connections for further analysis.

2. Agency Security Policy Enforcement: The contractor shall adhere to and support the ordering agency's security policy to ensure security regulations compliance. The contractor shall support agency's operational models and specific security rules. These shall be negotiated between the agency and the contractor. The contractor shall support adjustments to the agency's security strategy based on threats identified by the TIC Portal SOC. For example, adjustments to the security policy could be made by the agency's authorities after the SOC identifies changing trends in intrusion behavior.

3. Forensic Analysis: The contractor shall support full, real-time, header and payload, raw packet capture of selected agency's traffic flows and shall support subsequent forensic traffic analysis of cyber incidents as required by the agency (administrative, legal, audit or other operational purposes). The agency will identify technical requirements such as, but not limited to traffic of interest (relevant traffic to capture). The agency will require support to engineering parameters applied to the traffic capture such as, but not limited to packet capture rate and data retention period (e.g., 5% of the agency's traffic traversing the TIC Portal for a period of 60 days).
4. Custom Reports: The contractor shall provide reports as required by the ordering agency, including ad-hoc reports.
5. Agency NOC/SOC Console: The contractor shall provide additional features and functions customized to agency's specifications not covered by the Web portal included in the basic service.
6. Custom Security Assessment and Authorization Support (formerly known as Certification & Accreditation (C&A)): Agencies opting for security controls more stringent than the NIST High-Impact Baseline will negotiate agency-unique requirements directly with the contractor.
7. External Network Connection: The contractor shall enable the agency to connect to external IP networks at their physical locations. The traffic exchanged shall be IP traffic only and compliant to TIC portal's interconnecting requirements. The TIC portal shall support dedicated external connections to external partners (e.g., non-TIC federal agencies, externally connected networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but not limited to, permanent VPN over external connections, including the Internet, and dedicated private line connections to other external networks. The following baseline capabilities shall be supported for external dedicated VPN and private connections implemented using communication services offered through this contract, i.e. private lines or other dedicated connections SONETS, E-LINE, VPNS, etc. at the TIC portal:
    a) The connection shall terminate at an appropriate point so that traffic can be routed through the EINSTEIN Enclave to allow traffic to/from the external connections to be inspected. The EINSTEIN Enclave and the security stack at the portals are the public-facing side of the TIC Zone. The incoming traffic from the external network shall be inspected within the EINSTEIN Enclave and the security stack before reaching the internal network.

b) The connection shall terminate in front of the full suite of TIC sensors/capabilities to allow traffic to/from external connections to be inspected.

c) When connecting over the public networks including the Internet, the VPN connections shall be encrypted, compliant to NIST FIPS 140-2/3.

d) Connections terminated prior to routing through the EINSTEIN Enclave may use split tunneling. If required by the agency, the MTIPS contractor shall configure telecommunications service priority (TSP) for external connections, including to the Internet, to provide for priority restoration of telecommunication services.

e) The External Network Connection Feature is subject to performance measures established by EIS depending on the transport service selected for connectivity and included in Sections C and Section J.

8. Encrypted DMZ: The contractor shall support encryption, FIPS 140-2/3 compliant, from the agency's SDP at the edge of the agency's WAN to the MTIPS Portal. The contractor shall provide encryption devices and shall manage the devices.

9. Remote Access: The MTIPS portal shall support remote access for teleworkers connecting from home or satellite offices and mobile, on-the-go workers. Teleworkers and mobile workers are a subscriber agency's authorized staff who connect via ad-hoc Virtual Private Networks (VPNs) through external connections, including the Internet. For permanent VPN connections for branch offices or business partners use Feature 7 or 10 as appropriate. In addition to supporting the requirements of OMB M-06-16, "Protection of Sensitive Agency Information," the following baseline capabilities shall be supported for telework/remote access at the MTIPS portal:

a) The VPN connection shall terminate at an appropriate point prior to routing through the EINSTEIN Enclave and the full suite of TIC sensors/capabilities so that all outbound traffic to/from the VPN users to external connections, including the Internet, can be inspected within the EINSTEIN Enclave and the MTIPS portal security devices. In the case of outgoing traffic from the VPN users, the "Remote Access Enclave" shall connect to the aggregation devices located at the MTIPS transport interface before connecting to the portal's security stack and the EINSTEIN Enclave so that the outgoing traffic from the remote user/teleworker/mobile worker be inspected prior to reaching the Public Internet.

b) The VPN connection shall terminate in front of MTIPS-managed security controls including, but not limited to, a firewall and IDPS to allow traffic to/from remote access users to internal networks to be inspected.

c) All VPN connections shall be NIST FIPS 140-2/3 compliant.

d) The telework VPNS shall not be capable of split tunneling (see NIST SP 800-46 Rev1). Any VPN connection that allows split tunneling is considered an external connection, and terminates in front of the EINSTEIN Enclave.

e) The contractor shall use multi-factor authentication (see NIST SP 800-46 Rev1).

f) VPN concentrators and Virtual-Desktop/Application Gateways (Remote Access Enclave) shall use hardened appliances and shall be maintained in a separate network security boundary depending on the contractor's implementation.

g) Should telework/mobile worker remote clients use GFP, the VPN connection may use access at the IP network-level and access through specific Virtual Desktops/Application Gateways.

h) If telework/mobile worker remote clients use non-GFP, the VPN connection shall only use access through specific Virtual Desktops/Application Gateways.

i) Implementation requirements:

   i. The contractor shall support TLS and/or IPSec VPNs to connect to the MTIPS portals. The contractor shall provide the end device client (agent) if required by the agency.

   ii. The contractor shall support VPN Encryption Algorithm compliant to FIPS 140-2/3, i.e., 128-bit AES.

   iii. Multi-factor authentication services shall be supported, they include passwords and Cryptographic Tokens or PIVs

   iv. At the portal, the contractor shall build a separate DMZ (Remote Access Enclave) for Remote Access services to secure VPN concentrators and the rest of the infrastructure required to provide the service, e.g., Application Gateways, Virtualized Infrastructure, etc.

The contractor shall also support customized remote access implementations for teleworkers and mobile workers to meet agency-specific requirements.

10. Extranet Connections: The TIC portal shall support dedicated extranet connections to internal partners (e.g., TIC federal agencies, closed networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but not limited to, permanent VPN over external connections, including the Internet, and dedicated connections to other internal networks provided by communication services offered through this contract. The following baseline capabilities shall be supported for extranet dedicated VPN and private line connections at the TIC Portal:

   a) The connection shall terminate at an appropriate point before routing through the EINSTEIN Enclave and the full suite of TIC sensors/capabilities so that all outbound traffic to/from the extranet connections to external connections, including the Internet, is inspected within the EINSTEIN Enclave.

b) The connection shall terminate in front of the MTIPS-managed security controls including, but not limited to, a firewall and IDPS to allow traffic to/from extranet connections to internal networks, including other extranet connections, to be inspected.

c) VPN connections over shared public networks, including the Internet shall be NIST FIPS 140-2/3 compliant.

d) Split tunneling shall not be allowed unless directed otherwise from the ordering agency. (Agencies may authorize split tunneling in support of branch office and remote user solutions.) Any VPN connection that allows split tunneling is considered an external connection, and must terminate prior to routing through the EINSTEIN Enclave.

e) Implementation requirements:

   i. IPSec VPN from the fixed remote location (business partners, remote agency's sites, other agencies' sites, etc.) to the MTIPS portals.

   ii. Multi-Factor Authentication: Passwords, Cryptographic Tokens or PIV shall be supported.

   The contractor shall also support customized remote access implementations for extranet connections to meet agency-specific requirements.

11. Inventory/Mapping Service: The agency may request the MTIPS contractor to keep an inventory or a complete map of all networks connected to the MTIPS portal. The MTIPS contractor shall maintain a complete map, or other inventory, of all subscriber agencies' networks connected to the TIC access portal. The MTIPS contractor validates the inventory through the use of network mapping devices. Static translation tables and appropriate points of contact shall be provided to the CISA Incident Reporting System on a quarterly basis, to allow in-depth incident analysis.

C.2.8.4.3 Interfaces

The contractor shall support the UNIs at the SDP to connect to MTIPS Transport POP, as follows:

1. SONET Access as defined in Section C.2.9.1.4
2. Ethernet Access as defined in Section C.2.9.1.4

C.2.8.4.4 Performance Metrics

The performance levels and AQL of KPIs for MTIPS in Sections C.2.8.4.4.1 through C.2.8.4.4.2 are mandatory unless marked optional.

C.2.8.4.4.1 Performance Metrics for TIC Portal

KPI	User Type	Performance Standard (Level/Threshold)	AQL	How Measured
Av(TIC Portal)	Routine Critical	99.5%	≥ 99.5%	See Note 1
Grade of Service (Failover Time)	Routine	1 minute	≤ 1 minute	See Note 2
Grade of Service (Monitoring and Correlation	Routine	Real Time	≤ 4 hours 90% of the time	See Note 3
	Critical	Real Time	≤ 4 hours 99.9% of the time	
Grade of Service (Configuration/ Rule Change)	Routine	Within 5 hours for a Normal priority change	≤ 5 hours	See Note 4
		Within 2 hours for a Urgent priority change	≤ 2 hours	
EN (Firewall Security Event Notification)	Routine	Within 24 hours of a Low category event	≤ 24 hours	See Note 5
		Within 4 hours of a Medium category event	≤ 4 hours	
		Within 30 minutes of a High category event	≤ 30 minutes	
EN (Intrusion Detection/ Prevention Security Event Notification)	Routine	Within 24 hours of a Low category event	≤ 24 hours	See Note 5
		Within 10 minutes of a High category event	≤ 10 minutes	
Grade of Service (Virus Protection Updates and Bug Fixes)	Routine	Normal Priority Update 24 hours	≤ 24 hours	See Note 6
		Urgent Priority Update 2 hours	≤ 2 hours	

Notes:

1. The TIC Portal availability is calculated as a percentage of the total reporting interval time that all the TIC Portal components are operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Failover Time for the TIC Portal is the time that it takes to switch from one TIC Portal instance to another provided by the same contractor.
3. The GOS (Monitoring and Correlation) – The monitoring and correlation agents in the contractor's SOC shall detect a security event within 4 hours of its initiation at (a) 90% AQL for Routine, and (b) 99.9% AQL for Critical service levels. The monitoring and correlation systems shall provide real time fusion.
4. The GOS (Configuration/Rule Change) value represents the elapsed time between the configuration/change request and the change completion. The value is measured by logs/reporting. Changes are initiated and prioritized by the agency, or may be implemented in response to an event. Changes initiated by the contractor require agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency).
5. The Event Notification (EN) value represents the elapsed time between the detection of the event and the notification to the agency. Events are categorized as follows:

   a) Low – Events in the Low category have a negligible impact on service. They include incidents that do not significantly affect network security, as well as minor hardware, software and configuration problems.

   b) Medium – Events in the Medium category have a more serious impact on service, and may indicate a possible security breach, threat or attack attempt. They may also cause the service to operate in a degraded state.

   c) High – Events in the High category represent violations that severely impact service and operations. They indicate a true compromise of network security. These events also include major hardware, software, and configuration problems, which should be immediately reported via email, or telephone, as specified by the agency.

6. The GOS (Virus Protection Updates and Bug Fixes) represents the time between the release of the virus protection updates and bug fixes (patches), and their deployment. This indicator ensures automatic and timely delivery of updates/bug fixes.

C.2.8.4.4.2 Performance Metrics for MTIPS Transport Collection and Distribution

KPI	User Type	Performance Standard (Level/Threshold)	(AQL	How Measured
Av(Port)	Routine	99.95%	≥ 99.95%	See Note 1
	Critical	99.995%	≥ 99.995%	
Latency (CONUS)	Routine	60 ms	≤ 60 ms	See Note 2
	Critical	50 ms	≤ 50 ms	
GOS (Data Delivery Rate)	Routine	99.95%	≥ 99.95%	See Note 3
	Critical	99.995%	≥ 99.995%	
Time to Restore	Without dispatch	4 hours	≤ 4 hours	
	With dispatch	8 hours	≤ 8 hours	
EN(Security Incident Reporting)	Routine	Near real time	≤ 30 min	See Note 4

Notes:

1. Port availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the port is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. Latency is the average one-way time for IP packets to travel over the EIS core network. The Backbone Latency metric does not apply for DSL and Cable High Speed access methods.
3. Network packet delivery is a measure of IP packets successfully sent and received over the EIS core network.
4. Security incident reporting to the CISA Incident Reporting System must be performed in near real-time, congruent with NIST SP 800-61 Rev 2), not to exceed 30 minutes, from the time of detection.

C.2.8.4.5 MTIPS Security Requirements

The contractor shall ensure security requirements are met for the MTIPS as defined in the System Security Plan (see Section C.2.8.4.5.4), at a High impact level and shall support government security and authorization efforts. The contractor shall also support the government's efforts to verify that these standards are being met.

C.2.8.4.5.1 General Security Compliance Requirements

In providing services under this contract, the contractor shall be subject to all applicable federal and agency-specific IT security directives, standards, policies, and reporting requirements. The contractor shall comply with Federal Information Security Management Act (FISMA) associated guidance and directives to include Federal Information Processing Standards (FIPS), NIST SP 800 series guidelines (available at: http://csrc.nist.gov/), GSA IT security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of government IT. Compliance references shall include:

- Federal Information Security Management Act (FISMA) of 2002; (44 U.S.C. Section 301. Information Security) available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
- Federal Information Security Modernization Act of 2014; (to amend Chapter 35 of 44 U.S.C.) available at: https://www.congress.gov/113/bills/s2521/BILLS-113s2521es.pdf.
- Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996," available at: https://www.fismacenter.com/clinger%20cohen.pdf.
- Privacy Act of 1974 (5 U.S.C. § 552a).
- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and contractors," August 27, 2004; available at: http://www.idmanagement.gov/.
- OMB Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended; available at: http://www.whitehouse.gov/omb/circulars_a130_a130trans4/.
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies" (Available at: http://www.whitehouse.gov/omb/memoranda_2004).
- OMB Memorandum M-05-24, "Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors" (Available at

https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf.)

- OMB Memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors” (Available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf.)
- OMB Memorandum M-14-03, “Enhancing the Security of Federal Information and Information Systems” (Available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.)
- FIPS PUB 199, “Standards for Security Categorization of Federal Information and Information Systems”
- FIPS PUB 200, “Minimum Security Requirements for Federal Information and Information Systems”
- FIPS PUB 140-2, “Security Requirements for Cryptographic Modules”
- FIPS PUB 140-3, “Security Requirements for Cryptographic Modules”
- NIST Special Publication 800-18 Revision 1, “Guide for Developing Security Plans for Federal Information Systems”
- NIST Special Publication 800-30 Revision 1, “Guide for Conducting Risk Assessments”
- NIST Special Publication 800-34 Revision 1, “Contingency Planning Guide for Federal Information Systems”
- IST SP 800-37 Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”
- NIST SP 800-39, “Managing Information Security Risk: Organization, Mission, and Information System View”
- NIST SP 800-41 Revision 1, “Guidelines on Firewalls and Firewall Policy”
- NIST SP 800-37 Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”
- NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems”

- NIST SP 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations”
- NIST SP 800-53A Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans”
- NIST SP 800-61 Revision 2, “Computer Security Incident Handling Guide”
- NIST SP 800-64, Revision 2, “Security Consideration in the System Developments Lifecycle”
- NIST SP 800-88 Revision 1, “Guidelines for Media Sanitization”
- NIST SP 800-128, “Guide for Security-Focused Configuration Management of Information Systems”
- NIST SP 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations”
- NIST SP 800-160 “Systems Security Engineering” dated November 2016
- NIST SP 800-161, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”
- Committee on National Security Systems (CNSS) Policy No. 12, National Information Assurance Policy for Space Systems Used to Support National Security Missions.
- Committee on National Security Systems Instruction 1253 (CNSSI No. 1253), Security Categorization and Control Selection for National Security Systems.

In addition to complying with the requirements identified in the government policies, directives and guides specified above, the contractor shall comply with the current GSA policies, directives and guides listed below (the current documents are referenced within the GSA IT Security Policy and are available upon request submitted to the GSA CO*)*:

- GSA Information Technology (IT) Security Policy, CIO P 2100.1(J).
- GSA Order CIO P 2181.1 “GSA HSPD-12 Personal Identity Verification and Credentialing Handbook”
- GSA Order CIO 2104.1, “GSA Information Technology (IT) General Rules of Behavior”
- GSA CIO P 1878.1, “GSA Privacy Act Program”
- GSA CIO P 1878.2A, “Conducting Privacy Impact Assessments (PIAs) in GSA”

- GSA IT Security Procedural Guide 01-01, “Identification and Authentication”
- GSA IT Security Procedural Guide 01-02, “Incident Response”
- GSA IT Security Procedural Guide 01-05, “Configuration Management”
- GSA IT Security Procedural Guide 01-07, “Access Control”
- GSA IT Security Procedural Guide 01-08, “Audit and Accountability Guide”
- GSA IT Security Procedural Guide 05-29, “IT Security Training and Awareness Program”
- GSA IT Security Procedural Guide 06-29, “Contingency Planning”
- GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk”
- GSA IT Security Procedural Guide 06-32, “Media Protection Guide”
- GSA IT Security Procedural Guide 07-35, “Web Application Security Guide”
- GSA IT Security Procedural Guide 08-39, “FY 2014 IT Security Program Management Implementation Plan”
- GSA IT Security Procedural Guide 10-50, “Maintenance Guide”
- GSA IT Security Procedural Guide 11-51, “Conducting Penetration Test Exercise Guide”
- GSA IT Security Procedural Guide 12-63, “GSA’s System and Information Integrity”
- GSA IT Security Procedural Guide 12-64, “Physical and Environmental Protection”
- GSA IT Security Procedural Guide 12-66, “Continuous Monitoring Program”
- GSA IT Security Procedural Guide 12-67, “Securing Mobile Devices and Applications Guide”
- GSA IT Security Procedural Guide 14-69, “SSL / TLS Implementation Guide”

C.2.8.4.5.2 Security Compliance Requirements

FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems,” is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in eighteen security-related areas. Contractor systems supporting the government must meet the minimum security requirements through the use of the security controls in accordance with NIST SP 800-53 Revision 4 (hereinafter described as NIST SP 800-53).

To comply with the federal standard, the government has determined the security category of the information and information system in accordance with FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," to be established at the High Impact Level and baseline security controls must be established as identified in NIST SP 800-53 and other associated directives and guides identified and/or provided by GSA. The contractor shall submit a Risk Management Framework Plan describing its approach for MTIPS security compliance. This plan shall be submitted with the proposal in accordance with NIST SP 800-37. (Reference: NIST SP 800-37 R1, and NIST SP 800-53 R4: SA-3, RA-3)

C.2.8.4.5.3 Security Assessment and Authorization (Security A&A)

The implementation of a new federal government IT system requires a formal approval process known as security A&A. NIST SP 800-37 Revision 1 (hereinafter listed as NIST SP 800-37) and GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk", provides guidance for performing the A&A process. The contractor's system shall have a valid security A&A (approved by GSA) prior to being placed into operation and processing government information. Failure to obtain and maintain a valid security A&A will be grounds for termination of the contract. The system must have a new security A&A conducted (and approved by GSA) at least every three (3) years, or when there is a significant change that impacts the system's security posture, or a system may qualify for ongoing security authorizations that are not time-limited (at the discretion of the Authorizing Official (AO)). All NIST SP 800-53 controls must be tested and assessed no less than every three (3) years unless otherwise determined by the AO.

C.2.8.4.5.4 System Security Plan (SSP)

The contractor shall comply with all security A&A requirements as mandated by federal laws, directives and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The level of effort for the security A&A is based on the System's NIST FIPS Publication 199 categorization. At a minimum, the contractor shall create, maintain and update the following security A&A documentation:

1. The SSP shall be completed in accordance with NIST SP 800-18 Revision 1 (hereinafter listed as NIST SP 800-18) and other relevant guidelines. The SSP shall also include, at a minimum, the following appendices consisting of required policies and procedures across 18 control families mandated per FIPS 200. The SSP for the information system shall initially be completed and submitted within 30 days of the NTP to include annual updates (Reference: NIST SP 800-53 R4: PL-2).

2. The contractor shall develop and maintain a Security Assessment Boundary and Scope Document (BSD) as identified in NIST SP 800-37. This document will be used to determine the actual security assessment boundary. The set of information resources allocated to an information system defines the boundary for that system. These resources support the same mission/business objectives or functions. Generally the set of information resources is located within the same operating environment; however, distributed systems can reside in various locations with similar operating environments. Establishing and/or changing information system security boundaries is a cooperative effort between the federal government and the industry partner(s). Key stakeholders within the federal government and its counterparts within the industry partner(s) include but are not limited to the following: Information System Owner, Chief Information Security Officer, Authorizing Official, and Information Systems Security Manager/Officer. A template is available in Section J.8. The BSD for the information system shall be completed and submitted within 15 days of the NTP (Reference: NIST SP 800-37 R1).
3. The contractor shall develop and maintain Interconnection Security Agreements (ISA) in accordance with NIST SP 800-47. The contractor shall provide any ISAs for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CA-3).
4. The contractor shall develop and maintain a GSA NIST SP 800-53 R4 Control Tailoring Workbook as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk”. A template is included in Section J.8. Column E of the workbook titled “Contractor Implemented Settings” shall document all contractor-implemented settings that are different from GSA-defined settings, and where GSA-defined settings allow a contractor to deviate. The contractor shall provide a Control Tailoring Workbook for the information system with the initial security A&A package (Reference: NIST SP 800-53 R4: AC-1).
5. The contractor shall develop and maintain a GSA NIST SP 800-53 R4 Control Summary Table for a High Impact Baseline as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” A template is provided in Section J.8. The contractor shall provide a GSA NIST SP 800-53 R4 Control Summary Table for the information system with the initial security A&A package (Reference: NIST SP 800-53 R4: AC-1).
6. The contractor shall develop and maintain a Rules of Behavior (RoB) for information system users as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk” and GSA Order CIO 2104.1, “GSA IT General Rules of Behavior”. The contractor shall provide an RoB for the information

system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: PL-4).

7. The contractor shall develop and maintain a System Inventory that includes hardware, software and related information as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk”. The contractor shall provide a System Inventory for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CM-8).

8. The contractor shall develop and maintain a Contingency Plan (CP) including Disaster Recovery Plan (DRP) and Business Impact Assessment (BIA) completed in agreement with NIST SP 800-34. The contractor shall provide a CP for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CP-2).

9. The contractor shall develop and maintain a Contingency Plan Test Plan (CPTP) completed in agreement with GSA IT Security Procedural Guide 06-29, “Contingency Planning.” The contractor shall provide an CPTP for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CP-4).

10. The contractor shall test the CP and document the results in a Contigency Plan Test Report (CPTR), in agreement with GSA IT Security Procedural Guide 06-29, “Contingency Planning.” The contractor shall provide a CPTR for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CP-4).

11. The contractor shall perform a Privacy Impact Assessment (PIA) completed as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk”. The contractor shall provide a PIA for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: AR-2, AR-3 and AR-4).

12. The contractor shall develop and maintain a Configuration Management Plan CMP) (Reference: NIST SP 800-53 control CM-9; NIST SP 800-128; GSA CIO-IT Security 01-05). The contractor shall provide a CMP for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CM-9).

13. The contractor shall develop and maintain a System(s) Baseline Configuration Standard Document (Reference: NIST SP 800-53 control CM-2; NIST SP 800-128; GSA CIO-IT Security 01-05). The contractor shall provide a well defined, documented, and up-to-date specification to which the information system is

built. The contractor shall provide the System Baseline Configuration for the information system as a part of the CMP with the initial security A&A package and provide annual updates (Reference: NIST SP 800-53 R4: CM-9).

14. The contractor shall develop and maintain System Configuration Settings (Reference: NIST SP 800-53 control CM-6; NIST SP 800-128; GSA CIO-IT Security 01-05). The contractor shall establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems shall be configured in accordance with GSA technical guides, NIST standards, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening systems, as deemed appropriate by the AO. System configuration settings shall be included as part of the CMP and shall be updated and/or reviewed on an annual basis (Reference: NIST SP 800-53 R4: CM-9).

15. The contractor shall develop and maintain an Incident Response Plan (IRP) (Reference: NIST 800-53 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02 “Incident Response”). The contractor shall provide an IRP for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: IR-8).

16. The contractor shall test the IRP and document the results in an Incident Response Test Report (IRTR) (Reference: NIST SP 800-53 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02 “Incident Response”). The contractor shall provide an IRTR for the information system with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: IR-3).

17. The contractor shall develop and maintain a Supply Chain Risk Management (SCRM) Plan. The contractor shall develop a SCRM Plan to reduce supply chain risks to performance and security of the contractor’s MTIPS throughout the contractor’s Muli-Agency TICAP solution life cycle. The contractor shall provide an SCRM Plan for the information system with its proposal to include annual updates (References: NIST SP 800-161 and NIST SP 800-53 R4: SA-12).

18. Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the contractor’s system and its environment of operation to determine if the security controls in the information system continue to be effective over time and as changes occur in the system and environment. The contractor shall develop and maintain a Continuous Monitoring Plan to

document how continuous monitoring of information system will be accomplished. Through continuous monitoring, security controls and supporting deliverables shall be updated and submitted to GSA per the schedules below. The submitted deliverables provide a current understanding of the security state and risk posture of the information systems. They allow GSA authorizing officials to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

19. The contractor shall develop and maintain a Plan of Action and Milestones completed in agreement with GSA IT Security Procedural Guide 06-30, “Plan of Action and Milestones (POA&M).” All scans associated with the POA&M shall be performed as an authenticated user with elevated privileges. Vulnerability scanning results shall be managed and mitigated in the POA&M and submitted together with the quarterly POA&M submission. (Reference: NIST SP 800-53 R4; RA-5 and GSA CIO-IT Security Guide 06-30). Scans shall include all networking components that fall within the security accreditation boundary. The appropriate vulnerability scans shall also be submitted with the initial security A&A package. An annual information system User Certification/Authorization Review shall be annotated on the POA&M (a POA&M template is provided in Section J.8). The contractor shall provide a POA&M for the information system as part of the initial security A&A package followed by quarterly updates after receipt of the ATO. Note: Critical and High vulnerabilities shall be updated monthly (Reference: NIST SP 800-53 R4; CA-5).

20. All FIPS 199 Low, Moderate and High impact information systems must complete an independent internal and external penetration test and provide an Independent Penetration Test Report documenting the results of vulnerability analysis and exploitability of identified vulnerabilities with security assessment package and on an annual basis in accordance with GSA CIO-IT Security Guide 11-51. GSA will provide for the scheduling and performance of these penetration tests. All penetration test exercises must be coordinated through the GSA Office of the Chief Information Security Officer (OCISO) Security Engineering (ISE) division at itsecurity@gsa.gov per GSA CIO-IT Security Guide 11-51. Applicable NIST SP 800-53 R4 Controls are CA-5 and RA-5.

21. All FIPS 199 Low, Moderate, and High impact information systems must conduct code analysis reviews in accordance with GSA CIO Security Procedural Guide 12-66 using the appropriate automated tools (e.g., Fortify, Veracode) to examine for common flaws, and document results in a Code Review Report to be submitted prior to placing system into production, when there are changes to

code and on an annual basis. Applicable NIST SP 800-53, R4 Control is SA-11. References: GSA CIO Security Procedural Guides 06-30, “Managing Enterprise Risk” and GSA CIO Security Procedural Guide 12-66, “Continuous Monitoring Program.” If applicable, a Code Review Report shall be submitted as an initial deliverable prior to placing the information system into production, when there are changes to code, and on an annual basis (Reference: NIST SP 800-53 R4: SA-11).

22. The government is responsible for providing the Security/Risk Assessment and Penetration Tests. The contractor shall allow GSA employees (or GSA designated third party contractors) to conduct security A&A activities to include control reviews in accordance with NIST SP 800-53/NIST SP 800-53A and GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk”. Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of government information. This includes the general support system infrastructure. All scans must be performed as an authenticated user with elevated privileges.

23. All identified gaps between required 800-53 controls and the contractor’s implementation as documented in the Security/Risk Assessment Report (SAR) shall be tracked by the contractor for mitigation in a POA&M document completed in accordance with GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” Depending on the severity of the gaps, the government may require them to be remediated before an Authorization to Operate (ATO) is issued.

24. The contractor shall mitigate all security risks found during the security A&A and continuous monitoring activities. All critical and high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The government will determine the risk rating of vulnerabilities. Updates on the status of all critical and high vulnerabilities that have not been closed within 30 days shall be provided on a monthly basis.

25. The contractor shall deliver the results of the annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26, “FISMA Implementation”. Each fiscal year the annual assessment will be completed in accordance with instructions provided by GSA (Reference: NIST SP 800-53 R4: CA-2).

26. Reserved

27. The contractor shall develop and keep current all policy and procedures documents, as outlined in the specified NIST documents as well as appropriate GSA IT Security Procedural Guides. The following documents shall be verified and reviewed during the initial security assessment and updates provided to the GSA COR/ISSO/ISSM biennially:

    a) Access Control Policy and Procedures (NIST SP 800-53 R4: AC-1)
    b) Security Awareness and Training Policy and Procedures (NIST SP 800-53 R4: AT-1)
    c) Audit and Accountability Policy and Procedures (NIST SP 800-53 R4: AU-1)
    d) Security Assessment and Authorization Policies and Procedures (NIST SP 800-53 R4: CA-1)
    e) Configuration and Management Policy and Procedures (NIST SP 800-53 R4: CM-1)
    f) Contingency Planning Policy and Procedures (NIST SP 800-53 R4: CP-1)
    g) Identification and Authentication Policy and Procedures (NIST SP 800-53 R4: IA-1)
    h) Incident Response Policy and Procedures (NIST SP 800-53 R4: IR-1)
    i) System Maintenance Policy and Procedures (NIST SP 800-53 R4: MA-1)
    j) Media Protection Policy and Procedures (NIST SP 800-53 R4: MP-1)
    k) Physical and Environmental Policy and Procedures (NIST SP 800-53 R4: PE-1)
    l) Security Planning Policy and Procedures (NIST SP 800-53 R4: PL-1)
    m) Personnel Security Policy and Procedures (NIST SP 800-53 R4: PS-1)
    n) Risk Assessment Policy and Procedures (NISTSP 800-53 R4: RA-1)
    o) Systems and Services Acquisition Policy and Procedures (NIST SP 800-53 R4: SA-1)
    p) System and Communication Protection Policy and Procedures (NIST SP 800-53 R4: SC-1)
    q) System and Information Integrity Policy and Procedures (NIST SP 800-53 R4: SI-1)

C.2.8.4.5.5 Additional Security Requirements

The contractor shall ensure that proper privacy and security safeguards are adhered to in accordance with the FAR Part 52.239-1, see Section I.

The deliverables identified in Section C.2.8.4.5.5 shall be labeled “CONTROLLED UNCLASSIFIED INFORMATION” (CUI) or contractor selected designation per document sensitivity. External transmission/dissemination of Controlled Unclassified Information (CUI) data to or from a GSA computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2/3, "*Security requirements for Cryptographic Modules.*"

Where appropriate, the contractor shall ensure implementation of the requirements identified in the FAR (see Section I, 52.224-1, "*Privacy Act Notification*" and FAR 52.224-2, "*Privacy Act.*")

The contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the federal government's agent.

The government has the right to perform manual or automated audits, scans, reviews, or other inspections of the contractor's IT environment being used to provide or facilitate services for the government. In accordance with the FAR (see Section I, 52.239-1) the contractor shall be responsible for the following privacy and security safeguards:

1. The contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the contractor under this contract or otherwise provided by the government (except for disclosure to a consumer agency for purposes of security A&A verification).
2. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the confidentiality, integrity and availability of any non-public government data collected and stored by the contractor. The contractor shall afford the government logical and physical access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods:
   - Authenticated and unauthenticated operating system/network vulnerability scans;
   - Authenticated and unauthenticated web application vulnerability scans;
   - Authenticated and unauthenticated database application vulnerability scans and
   - Internal and external penetration testing.
3. Automated scans can be performed by government personnel, or agents acting on behalf of the government, using government operated equipment, and government specified tools. If the contractor chooses to run its own automated scans and/or penetration tests, results from these scans and/or penetration tests may, at the government's discretion, be accepted in lieu of government

performed vulnerability scans and/or penetration tests. In these cases, scanning tools and their configurations shall be approved by the government. In addition, the results of contractor-conducted scans and/or penetration tests shall be provided, in full, to the government.

C.2.8.4.5.5.1 Personnel Background Investigation Requirements

The contractor shall perform personnel security / suitability checking in accordance with FAR Part 52.204-9 (see Section I).

All contractor personnel with access to the contracted system that is within the security A&A scope must successfully complete a background investigation in accordance with Homeland Security Presidential Directive-12 (HSPD-12), OMB guidance M-05-24, M-11-11, and as specified in GSA CIO Order 2100.1J and GSA Directive 9732.1D Suitability and Personnel Security to provide services under this contract. The required background investigations for administrative personnel shall be a minimum of a National Agency Check with Written Inquiries (NACI) and for technical staff shall be a Minimum Background Investigation (MBI) or higher depending upon their access and control over the systems. GSA will pay for any required background investigations for MTIPS.

C.2.8.5 Managed Security Service

C.2.8.5.1 Service Description

The array of services and technologies in the IT arena continues to expand as users and applications are added to agency networks. At the same time, cybercriminals and corrupt organizations are becoming ever more mobile and sophisticated. Therefore, agencies will continue to need managed security services to safeguard agency internal networks and systems against ever-evolving security threats.

Managed security services provide protection of endpoints, email, web, and networks, and include capabilities such as authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management.

C.2.8.5.1.1 Functional Definition

MSS comprises the following underlying functions:

1. Managed Prevention Service
2. Vulnerability Scanning Service
3. Incident Response Service
4. Trusted Internet Connections Service

These functions are described below:

Managed Prevention Service (MPS) provides the ability to monitor hosts and network traffic, and analyze network protocol and application activity to identify and mitigate suspicious activity. Supporting capabilities include managed firewalls, host- and network-based threat mitigation, as well as email- and DNS-based threat mitigation services.

Vulnerability Scanning Service (VSS) searches for security holes, flaws, and exploits on agency systems, networks and applications. The service tests for vulnerabilities by comparing scanned information to data contained in a database, which is updated as new threats are discovered. VSS can also simulate a real intrusion in a controlled environment, in order to gauge a network's susceptibility to attacks. The service performs external scans by remotely probing a network for vulnerabilities that generally come from the outside; and internal scans which detect flaws originating from the inside.

Incident Response Service (INRS) is comprised of both proactive and reactive activities. Proactive services are designed to prevent incidents. They include onsite consulting, strategic planning, security audits, policy reviews, vulnerability assessments, security advisories, and training. Reactive services involve telephone and on-site support for monitoring and analyzing alert information and responding to malicious events such as Denial of Services (DoS) attacks; virus, worm, and Trojan horse infections; illegal inside activities, espionage, and compromise of sensitive internal agency databases. INRS provides an effective method of addressing these security intrusions, thereby ensuring operational continuity in case of attacks. In addition, INRS provides forensics services that can assist in apprehending and prosecuting offenders.

Trusted Internet Connections Service (TICS) provides a networking and cybersecurity solution meeting the guidance provided by OMB and the Cybersecurity and Infrastructure Security Agency (CISA) for the TIC program. The OMB M-19-26 memorandum supersedes previous TIC guidance and provides an enhanced approach for implementing the TIC initiative while providing agencies with increased flexibility to use modern connectivity and data security capabilities. The memorandum also establishes a process for ensuring the TIC initiative is agile and responsive to advancements in technology and rapidly evolving threats. As a result agencies have been given more autonomy to decide how they can provide their workforce access to applications, data, and Internet access within their enterprises regardless of location. Although TICS solutions are to remain coordinated with the CISA NCPS and CDM programs, neither GSA nor CISA will be issuing formal authorization stating a TICS solution is compliant with OMB M-19-26 and the CISA TIC program office guidance. TICS solutions leveraged by an agency are to follow and comply with the customer agency specific Assessment and Authorization (A&A) processes while adhering to the CISA program guidance and other required National Policy Requirements in C.1.8.8.

CISA has issued Trusted Internet Connections 3.0 guidance to include a Program Guidebook, Reference Architecture, Security Capabilities Catalog, a Use Case Handbook, and an Overlay Handbook. The guidance and use case documents are living documents and will evolve as the related landscape changes.

The MSS TIC Service within the EIS contract relies on the CISA TIC program guidance documents. TICS solutions under this service shall adhere to the CISA guidance.

MSS TICS Solutions for the Cloud, Agency Branch Office, and Remote Users Initial Common TIC Use Cases listed in OMB M-19-26 may be constructed in a number of ways under EIS. Leveraging the SDWANS, MSS, MNS, SaaS, BIS, and other EIS services while following the CISA TIC guidance will produce a safe, flexible, and repeatable TICS solution for the agency which address the TIC 3.0 Security objectives listed below.

For the TIC 3.0 Traditional TIC use case, MTIPS based on the previous TIC 2.2 guidance may be proposed in combination with other Managed Security Services (MSS), Software as a Service (SaaS), Managed Network Services (MNS), or other EIS services to fill in any security capability gaps between a TIC 2.2 and a TIC 3.0 solution.

Objective	**Description**
Manage Traffic	Observe, validate, and filter data connections to align with authorized activities; least privilege and default deny
Protect Traffic Confidentiality	Ensure only authorized parties can discern the contents of data in transit; sender and receiver identification and enforcement
Protect Traffic Integrity	Prevent alteration of data in transit; detect altered data in transit
Ensure Service Resiliency	Promote resilient application and security services for continuous operation as the technology and threat landscape evolve
Ensure Effective Response	Promote timely reaction and adapt future response to discovered threats; policies defined and implemented; simplified adoption of new countermeasures

C.2.8.5.1.2 Standards

MSS shall comply, at a minimum, with the following standards:

1. FISMA (44 U.S.C. Section 301. Information security) available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
2. NIST FIPS PUB 140-2 – Security Requirements for Cryptographic Modules
3. NIST FIPS PUB 140-3 – Security Requirements for Cryptographic Modules
4. NIST FIPS PUB 199 – Standards for Security Categorization of Federal Information and Information Systems
5. NIST SP 800-40 – Guide to Enterprise Patch Management Technologies
6. NIST SP 800-41 – Guidelines on Firewalls and Firewall Policy
7. NIST SP 800-45 – Guidelines for Electronic Mail Security
8. NIST SP 800-51 – Guide to Using Vulnerability Naming Schemes
9. NIST SP 800-61 – Computer Security Incident Handling Guide
10. NIST SP 800-81-2 – Secure Domain Name System (DNS) Deployment Guide
11. NIST SP 800-83 – Guide to Malware Incident Prevention and Handling for Desktops and Laptops
12. NIST SP 800-92 – Guide to Computer Security Log Management
13. NIST SP 800-94 – Guide to Intrusion Detection and Prevention Systems
14. NIST SP 800-122 – Guide to Protecting the Confidentiality of Personally Identifable Information (PII)
15. NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
16. NIST Interagency Report 7802 – Trust Model for Security Automation Data (TMSAD) Version 1.0
17. CISA Incident Reporting Systemreporting requirements
18. IETF - Request for Comments (IETF-RFC) 2350 Expectations for Computer Security Incident Response
19. All new versions, amendments, and modifications of the above
20. All appropriate standards for any applicable underlying EIS access and transport services

C.2.8.5.1.3 Connectivity

MSS shall connect to and interoperate with the agency networking environment, including Demilitarized Zones (DMZs) and secure LANs, as required by the agency. The service shall also support connectivity to extranets and the Internet.

C.2.8.5.1.4 Technical Capabilities

The MSS capabilities, as defined in the following Sections C.2.8.5.1.4.1 through C.2.8.5.1.4.3 are mandatory unless marked optional.

C.2.8.5.1.4.1 Managed Prevention Service (MPS)

1. The contractor shall provide design and implementation services. This will enable the agency and the contractor to discuss matters such as system recommendations, a baseline assessment, rules, signature sets, configurations, and escalation procedures.
2. The contractor shall provide software and hardware components, including log servers, as applicable.
3. The contractor shall implement hardware or software load balancing capabilities and redundancy necessary to meet KPI and agency requirements.
4. The contractor shall provide installation support to include testing of equipment, testing of software, and loading of any agency-relevant data, as required by the agency.
5. The contractor shall maintain the latest configuration information for restoration purposes, reporting, and forensics analysis.
6. The contractor shall maintain the managed service capabilities, performing hardware/software upgrades and replacements, and content updates.
7. The contractor shall ensure that MPS systems and components comply with NIST SP 800-53 identification and authentication controls for high impact systems (FIPS 199). Administrative access devices requires multi-factor authentication (OMB M-11-11).
8. The contractor shall notify the agency about patches and bug fixes as soon as they become available.
9. The contractor shall test and deploy the latest patches and bug fixes as soon as they become available and are approved by the agency.
10. The contractor shall perform and document configuration and management as applicable to ensure that security, access, and information-flow policies are enforced as requested by the agency.
11. The contractor shall proactively monitor the health and status of MPS hardware/software components on a 24x7 basis for indications of compromise such as intrusions, anomalies, malicious activities, and network misuse.
12. The contractor shall monitor the overall performance of the service, including the adequacy of the hardware/software components as the network expands.
13. The contractor shall ensure the service allows only necessary functionality, network protocols, ports or services with documented customer approval.

14. The contractor shall perform and document periodic validation activities (e.g., via scans) to ensure service configurations are not vulnerable and are enforcing agency policies.
15. The contractor shall notify the agency of MPS-failure events via email, fax, or telephone, as directed by the agency.
16. The contractor shall be able to receive, handle, and use sensitive but unclassified cybersecurity indicators provided by the agency or the Department of Homeland Security (DHS).
17. The contractor shall ensure that service statistics, events messages, logs, and suspected attack information are sent via secure means to the agency-specified operation center.
18. The contractor shall ensure that event messages associated with DHS-provided indicators are sent via secure means to DHS.
19. The contractor shall ensure that event messages have necessary and consistent timestamps and content to establish context including, as appropriate, date/time of occurance (including time zone); related indicators, policies, and anomalies; source and destination addresses, ports, and protocols; operating system, processes, and application; detection source and location.
20. The contractor shall be able to identify and retrieve each customer agency's data for the agency, without divulging any other agency's data.
21. The contractor shall provide the agency with secure web access to logs and service information including the following:
    a) Active Sessions
    b) Port and Protocol Activity
    c) Authentication Statistics
    d) Connections/Attempts counts and results (accepted/rejected) by port
    e) Events, rule violations, and attacks detected including name,description, level, impact date, time, vulnerabilities and targeted weakness, and remedies
    f) Source and Destination IP Addresses, domains (fully-qualified domain name) and URLs; as well as statistics
    g) Affected endpoints
    h) Managed Prevention Service Statistics and Utilization
    i) Outages
    j) Configuration Modifications
    k) Change Requests and Event Tickets

C.2.8.5.1.4.2 Vulnerability Scanning Service (VSS)

The contractor shall support the agency in establishing, implementing and maintaining a vulnerability scanning service, which shall be operational on a 24x7 basis. The service shall provide the following:

1. External Vulnerability Scanning which tests Internet-connected nodes in the network, including web environments.
2. Internal Vulnerability Scanning which looks for local/host flaws and internal threats, usually inside the firewall.

The service shall periodically probe networks, including operating systems and application software, for potential openings, security holes, and improper configuration.

The service shall probe agency systems for vulnerabilities in, but not limited to, the following areas:

1. Back doors
2. Bind
3. Browser
4. Brute Force Attacks
5. Common Gateway Interface - Binary (CGI-Bin)
6. Daemons
7. Distributed Component Object Model (DCOM)
8. Databases
9. Domain Name Service (DNS)
10. eCommerce Applications
11. Email
12. Firewalls
13. File Sharing
14. FTP
15. General Remote Services
16. Hardware and Network Appliances
17. Hubs
18. Information/Directory Services
19. Instant Messaging
20. Lightweight Directory Access Protocol (LDAP)
21. Mail Applications
22. Multimedia Internet Mail Extension (MIME)

23. Network
24. Network Sniffers
25. Netbios
26. Network File System (NFS)
27. Network Information System (NIS)
28. OS Critical Issues
29. OS Groups
30. OS Networking
31. OS Password Checks
32. OS Policy Issues
33. OS Registry
34. OS Services
35. OS Users
36. Port Scans
37. Protocol Spoofing
38. Router-Switch
39. Remote Procedure Call (RPC)
40. Shares
41. Simple Mail Transfer Protocol (SMTP)
42. Simple Network Management Protocol (SNMP)
43. Server Message Block (SMB)
44. Transmission Control Protocol / Internet Protocol (TCP/IP)
45. Trojan Horses
46. Web Scans
47. Web Servers
48. Wireless Access Points

The contractor shall:

1. Proactively identify network vulnerabilities and propose appropriate countermeasures, fixes, patches, and workarounds.
2. Notify the agency of vulnerabilities discovered via email, fax, or telephone, as directed by the agency.
3. Provide the agency with secure Web access to vulnerability information, scan summaries, device/host reports, and trend analyses.

4. Review vulnerabilities discovered with the agency, as required.
5. Provide scan scheduling flexibility to the agency in order to minimize any interruptions in normal business activities.
6. Provide the agency with non-destructive and non-intrusive vulnerability scans that will not crash the systems being analyzed or disrupt agency operations. The scans shall not provoke a denial of service condition on the agency system being probed.
7. Use other analytical means to ascertain the vulnerability of agency systems if a particular scan is potentially destructive or intrusive.
8. Ensure that the scanning engine is regularly updated with new vulnerabilities information in order to maintain effectiveness of the service.
9. Support networks of varying size and complexity.

C.2.8.5.1.4.3 Incident Response Service (INRS)

1. The contractor shall review the agency’s security infrastructure and develop appropriate strategic plans in collaboration with the agency. These plans shall detail the incident response process, identify internal resources, assign duties to team members, describe policies, define severity levels, list escalation chains, and specify emergency/recovery procedures.
2. The contractor shall provide the agency with effective incident response support on a 24x7 basis.
3. The contractor shall maintain a problem detection system for the diagnosis of alerts and violations.
4. The contractor shall analyze suspicious security alerts to determine the significance and scope of an event and immediately notify the agency when the event is deemed high priority.
5. The contractor shall provide the agency with immediate access to vulnerability and severe alert information, which shall contain but not be limited to the following: Description, Target, Origin, Potential Incident Impacts, Remedies, Prevention Measures.
6. The contractor shall coordinate with the agency to handle potential security incidents according to the appropriate response procedures.
7. The contractor shall provide countermeasures to contain the security incident, limit its spread, and protect internal systems.
8. The contractor shall recommend the fixes necessary to eliminate identified vulnerabilities, and appropriate procedures to guard against future attacks.
9. The contractor shall provide the agency with secure web access to incident analysis findings and recommendations.

10. The contractor shall assist the agency in containing the damage and restoring affected systems to their normal operational state.
11. The contractor shall assist the agency in testing restored systems in order to ensure that identified vulnerabilities have been corrected.
12. The contractor shall provide dedicated support until resolution of the problem.
13. The contractor shall provide post-incident investigative and forensics services. This includes isolating the impacted area, capturing and collecting data, categorizing malicious or illegal events, and performing reconstruction analyses. The contractor shall handle and preserve the data collected according to sound scientific and evidence rules, as the information may serve as evidence in administrative actions and legal proceedings. The contractor shall trace the offenders and assist in prosecuting attackers, as required.
14. The contractor shall provide telephone support to the agency, as required.
15. The contractor shall deploy cybersecurity personnel to agency sites to handle security incidents, as necessary.
16. The contractor shall provide security awareness training to agency personnel as required. This includes mock attack drills, emerging threats and vulnerabilities workshops, and new incident response tools and processes demonstrations. The frequency and nature of training activities may vary according to agency needs.

C.2.8.5.1.4.4 Trusted Internet Connections Service (TICS)

1. The contractor shall provide TICS solutions that adhere to the current DHS CISA Trusted Internet Connections (TIC) guidance.

2. The contractor shall ensure their TICS solutions adhere to the Key Concepts of TIC 3.0 and the Conceptual Implementation of TIC 3.0 listed in the CISA Trusted Internet Connection Reference Architecture (Volume 2) guidance.

3. The contractor shall ensure their TICS solutions contain the required Security Objectives and Security Capabilities listed in the CISA Trusted Internet Connections Security Capabilities Catalog (Volume 3) guidance.

    a. TICS solutions shall include the defined Universal Security Capabilities: Enterprise-level capabilities that outline guiding principles for TIC use cases.

    b. TICS solutions shall include the defined Policy Enforcement Point Security Capabilities: Network-level capabilities that inform technical implementation for relevant TIC use cases.

4. The contractor shall reference the CISA TIC Use Case Handbook (Volume 4) TIC 3.0 Use Case Structure when designing and providing a TICS solution to the

EIS customer. The Use Case Handbook outlines alternative security controls, such as endpoint and user-based policy enforcment point protections, that must be in place for specific instances where traffic is not required to flow through a traditional TIC 2.2 access point (i.e. TICAP or MTIPS).

5. The contractor shall reference the CISA TIC Overlay Handbook (Volume 5) guidance when constructing and proposing TICS solutions for the ordering agency customer. The Overlay Structure is a high level mapping of a contractor's proposed TICS solution to the list of deployable security controls, security capabilities, and best practices within the Security Capabilities Catalog (Volume 3) of the CISA TIC Core Guidance. The Overlay will assist agency customers with identifying any gaps in the proposed TICS solution as it maps to the Security Objectives and Security Capabilities from the CISA TIC Core and Use Case Guidance documentation. Some proposed TICS solutions may not align with all the recommended TIC security capabilities for the intended use case, and agencies may need to obtain additional Managed Security Services from the EIS provider or other third-party providers to secure their environments to the use case specifications and their agency specific requirements.
6. The contractor proposed TICS solutions shall integrate with and support the CISA NCPS and CDM program requirements as required by the agency customer. Consult the NCPS Program and CDM Program references for further details.

C.2.8.5.2 Features

The following MSS features are mandatory unless marked optional.

1. Managed Prevention Service:

   a) Firewall – The contractor shall provide, operate and manage hardware and software components to analyze packet headers and enforce policy based on protocol type, source address, destination address, source port, and/or destination port. The managed firewall solutions shall apply stateful protocol analysis to compare traffic to generally accepted definitions of benign protocol activity and identify deviations. The firewall will provide Network Address Translation (NAT) and Port Address Translation (PAT) in order to disguise internal IP addresses, and it shall enforce agency-specified security policies by blocking packets and terminating sessions that violate those policies.

   b) Personal Firewalls – The contractor shall provide personal firewalls or personal firewall appliances in order to secure remote personal computers or small remote networks (i.e., home offices), as required by the agency

c) Network Intrusion Prevention System – The contractor shall provide an in-line deep-packet capability to monitor network traffic (HTTP/S, FTP, etc.), analyze network and application protocol activity and content to identify and mitigate suspicious activity, and block or disrupt activity based on signatures and behavor.

d) Endpoint Protection – The contractor shall provide host-based intrusion prevention capabilities, including application firewall, endpoint recording, threat detection, whitelisting, banning, and remediation in order to protect agency endpoints.

e) Secure Web Proxy – The contractor shall provide an intermediary between endpoints allowing URL- and domain-based filtering as well as obfuscation of internal IP addresses. The contractor shall support URL blocking.

f) Inbound Web Filtering – The contractor shall provide the ability to filter inbound web sessions to web servers at the HTTP/HTTPS/SOAP/XML-RPC/Web Service application layers from, but not limited to, cross site scripting (XSS), SQL injection flaws, session tampering, buffer overflows and malicious web crawlers.

g) Application-Level Gateway – The contractor shall provide an intermediary between endpoints allowing for application layer control/data protocols (FTP, SIP, IM, etc.) to be proxied.

h) Network Behavior Analysis – The contractor shall provide a capability that develops a profile of 'normal' agency behavior and examines network traffic (including encrypted sessions) to identify threats that generate unusual traffic flows, such as DDoS attacks, scanning, and certain forms of malware. The contractor shall perform anomaly detection in order to identify atypical traffic trends and unusual behaviors that may indicate a potential attack. The contractor shall keep logs of at least the source, destination and size of the encrypted connections for further analysis.

i) Network Traffic Content Analysis and Sandboxing – The contractor shall provide capabilities that extract objects from network traffic and examine those objects using real-time binary and execution engine analysis.

j) Email Forgery Protection and Filtering – The contractor shall provide capabilities for inbound and outbound forgery protection (domain-level sender forgery analysis equivalent to Domain Keys Identified Mail or Sender Policy Framework standards, digital signing procedures for outgoing email messages to ensure that they have been digitally signed at the domain level), as well as domain and header-based filtering, phishing and spam filtering, block attachments violating policy (e.g., size, file type), sanitize malicious content and quarantine messages, as well as measures that can conceal, limit, or change information about the agency's networks or domains, reducing visibility to outsiders.

k) Email Content Analysis and Sandboxing – The contractor shall provide capabilities that extract objects from email traffic and examine those objects using real-time binary and execution engine analysis.

l) User Authentication Integration - The contractor shall support the integration of the email-based threat mitigation service with the agency's own authentication service, as specified by the agency. Examples include Kerberos, Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory, Remote Authentication Dial-In User Service (RADIUS),RSA SecureID, Terminal Access Controller Access Control System (TACACS), Extended TACACS (XTACACS), or TACACS+.

m) DNSSEC – The contractor shall provide DNS security capabilities described in NIST SP800-81-2 to ensure data integrity and source authentication.

n) DNS Sinkholing – The contractor shall provide capabilities to block or redirect network traffic based on manipulation of DNS query responses.

o) Data Loss Prevention – The contractor shall provide capabilities to discover and identify sensitive data and to manage, monitor, and protect it from being deleted, destroyed or divulged.

p) Demilitarized Zones (DMZs) Support – The contractor shall support connections to Demilitarized Zones (DMZs) which serve as buffers between the agency’s private networks and outside public networks. DMZs can apply to Web (HTTP), FTP, email (SMTP), and DNS servers.

q) Extranet Support – The contractor shall support connections to extranets which can facilitate inter-agency interactions or enable the agency to interface with trusted stakeholders.

r) Firewall-to-Firewall VPNs – The contractor shall support firewall-to-firewall VPNs which establishes secure tunnels between agency firewalls, and also between firewalls and the contractor’s operation center.

s) Remote Client VPNs – The contractor shall provide remote agency users with secure access to the network, employing VPN encryption technology.

t) EINSTEIN 2 – The contractor shall interact with DHS to obtain indicators, establish USCERT event feeds, and provide EINSTEIN network flow and detection capabilities for agency-specified traffic.

u) Short-Term Storage – The contractor shall provide storage capacity to retain at least 24 hours of agency-specific data generated by the MPS. Traffic shall be selectively filtered and stored, and retained data shall be made securely available to the agency.

v) Long-Term Storage – The contractor shall provide storage capacity to retain a year of agency-specific data generated by the MPS. Traffic shall be selectively filtered and stored, and retained data shall be made securely available to the agency.

w) Agency-specified policy enforcement.

2. Vulnerability Scanning Service (VSS):

   a) VSS API: The contractor shall provide the agency with the ability to integrate the service into its own tools and applications, using for example, a standard XML and RESTful APIs, as required by the agency. This will assist in-house security personnel with tasks such as scanning IP addresses, assessing host vulnerabilities, creating user accounts, and exporting vulnerability data.

3. Incident Response Service (INRS)

   a) Advanced Analytics. The contractor shall provide and apply various statistical techniques from the modeling, machine learning, and data mining disciplines to analyze relevant observations for threat discovery, assessment, situational awareness, and prediction. Where applicable, the techniques provided must yield confidence intervals establishing the statistical significance of findings. When statistical significance cannot be established using rigorous, state-of-the-art techniques, the findings must include this caveat.

4. Trusted Internet Connections Service (TICS)

   a) Encrypted Traffic: The TICS solution shall monitor, scan and filter the incoming and outgoing encrypted traffic traversing agency Web Security Capabilities Policy Enforcement Points based on URL or IP address. The TICS solution shall analyze all encrypted traffic that passes through the Web Security Capabilities PEP for suspicious patterns that might indicate malicious activity and shall retain the logs of at least the source, destination and size of the encrypted connections for further analysis. Log retention time frames shall be specified within the agency requirements.

   b) Agency Security Policy Enforcement: The contractor shall adhere to and support the ordering agency's security policy to ensure security regulations compliance. The contractor shall support agency's operational models and specific security rules. These shall be negotiated between the agency and the contractor. The contractor shall support adjustments to the agency's security strategy based on threats identified. For example, adjustments to the security policy could be made by the agency's authorities after the SOC identifies changing trends in intrusion behavior.

   c) Forensic Analysis: The contractor shall support capturing and logging of traffic flows and shall support subsequent forensic traffic analysis of cyber incidents as required by the agency (administrative, legal, audit or other operational purposes). The agency shall identify technical requirements such as, but not limited to traffic of interest (relevant traffic to capture/log) and the data retention timelines required.

d) Custom Reports: The contractor shall provide reports as required by the ordering agency, including ad-hoc reports.

e) CISA NCPS Program Protections – At the appropriate TICS Policy Enforcement Points the contractor shall meet applicable routing requirements in Section C.1.8.8 ensuring encrypted connections are applied between agency Service Delivery Points, TICS aggregation points, and Policy Enforcement Points and the required data from the NCPS program is trasmitted to CISA for NCPS program data collection and inspection (i.e. to EINSTEIN, the Cloud Log Aggregation Warehouse (CLAW), etc.).

f) Custom Security Assessment and Authorization (A&A) Support (formerly known as Certification & Accreditation (C&A)): Agencies will specify agency-unique requirements and support required for A&A activities directly with the contractor.

g) External Network Connections: The contractor shall enable the agency to connect to external IP networks. The traffic exchanged shall be compliant with customer agency interconnecting requirements. The TICS solution shall support external connections to external partners (e.g., cloud service providers, non-TIC federal agencies, externally connected networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but not limited to, ad-hoc or permanent VPN over external connections, including the Internet, and dedicated private line connections to other external networks. The following baseline capabilities shall be supported for external connections implemented using communication services offered through this contract, i.e. ETS, IPS, VPNS, BIS, CHS, PLS, SDWANS, etc or other dedicated connections at the TICS solution location(s):

1. The connection shall terminate at an appropriate point so that traffic can be routed through the required Policy Enforcement Points to allow traffic to/from the external connections to be inspected. The incoming traffic from the external network shall be inspected within the Policy Enforcement Points before reaching the internal network while ensuring compliance with CISA NCPS program requirements.
2. When connecting over the public networks including the Internet, the connections shall be encrypted, compliant to NIST FIPS 140-2/3.
3. Connections terminated prior to routing through the Policy Enforcement Point (PEP) may use split tunneling, while ensuring compliance with CISA NCPS requirements.
4. The External Network Connection Feature is subject to performance measures established by EIS depending on the

transport service selected for connectivity and included in Sections C and Section J.

h) The contractor shall support FIPS 140-2/3 compliant encryption within their TICS solutions. The contractor shall provide the encryption capability and shall manage the capability where required by the customer.

i) (OPTIONAL) Remote Access: The TICS solution shall support remote access for teleworkers connecting from home or satellite offices and mobile, on-the-go workers. Teleworkers and mobile workers are a subscriber agency's authorized staff that connects through external connections, including the Internet. In addition to supporting the requirements of OMB M-06-16, "Protection of Sensitive Agency Information," the following baseline capabilities shall be supported for telework/remote access at the TICS solution policy enforcement points:

1. The connection shall terminate at an appropriate point prior to routing through the TICS Policy Enforcement Points (PEPs) so that all outbound traffic to/from the external connections, including the Internet, can be inspected within the TICS Policy Enforcement Points while ensuring compliance with CISA NCPS program requirements.
2. The external or remote connection shall terminate in front of TICS Policy Enforcement Point security controls including, but not limited to, a firewall and IDPS to allow traffic to/from remote access users to internal networks to be inspected.
3. All external or remote connections shall be NIST FIPS 140-2/3 compliant.
4. The VPN or remote connection shall not be capable of split tunneling (see NIST SP 800-46 Rev1). Any VPN connection that allows split tunneling is considered an external connection, and terminates in front of the Policy Enforcement Point (PEP) for inspection while also ensuring CISA NCPS program complaince.
5. The contractor shall use multi-factor authentication (see NIST SP 800-46 Rev1).
6. VPN concentrators and Virtual-Desktop/Application Gateways shall use hardened appliances and shall be maintained in a separate network security boundary depending on the contractor's implementation.
7. Implementation requirements:
    i. The contractor shall support TLS and/or IPSec VPNs or remote connections to connect to the TICS solutions where

applicable. The contractor shall provide the end device client (agent) if required by the agency.

- ii. The contractor shall provide a VPN or remote connection Encryption Algorithm compliant with FIPS 140-2/3.
- iii. Multi-factor authentication services shall be supported and issued in accordance to the NIST SP 800-63 Digital Identity Guidelines and agency specific requirements.
- iv. The contractor shall also support customized remote access implementations for teleworkers and mobile workers to meet agency-specific requirements.

j) Extranet Connections: The TICS solution shall support dedicated extranet connections to internal partners (e.g., partner federal agencies, closed networks at business partners, state/local governments) with a documented mission requirement and approval. This includes, but is not limited to, permanent VPN over external connections, including the Internet, and dedicated connections to other internal networks provided by communication services offered through this contract. The following baseline capabilities shall be supported for extranet dedicated connection, other tunneled traffic, and private line connections:

1. The connection shall terminate at an appropriate point before routing through the full suite of TICS Policy Enforcement Point (PEP) sensors/capabilities so that all outbound traffic to/from the extranet connections to external connections, including Internet transport, is inspected within the Policy Enforcement Point while ensuring compliance with CISA NCPS program requirements.
2. The connection shall terminate in front of the TICS policy enforcement point(s) to allow traffic to/from extranet connections to internal networks, including other extranet connections, to be inspected.
3. Extranet connections over shared public networks, including the Internet shall be NIST FIPS 140-2/3 compliant.
4. Split tunneling shall not be allowed, unless there is direction received from the agency customer to support split tunneling.
5. Implementation requirements:
   - i. VPN from the fixed remote location (business partners, remote agency's sites, other agencies' sites, etc.) to the TICS policy enforcement points.
   - ii. Multi-Factor Authentication: Passwords, Cryptographic Tokens or PIV shall be supported.

iii. The contractor shall also support customized remote access implementations for extranet connections to meet agency-specific requirements.

k) Additional EIS services shall be proposed to fill any CISA TIC 3.0 Security Capabilities Catalog (Volume 3) gaps to the customer requirements for a particular agency requested TICS use case. The CISA Overlay Guidance (Volume 5) will aid the contractor in identifying the Security Capabilities Catalog gaps where additional EIS services may be required.

C.2.8.5.3 Interfaces

MSS shall support the following services:

1. VPNS as specified in Section C.2.1.1
2. ETS as specified Section C.2.1.2
3. IPS as specified in Section C.2.1.7
4. BIS as specified in Section C.2.1.8
5. SDWANS as specified in Section C.2.8.10

C.2.8.5.4 Performance Metrics

The MSS performance levels and AQL of KPI in Section C.2.8.5.4.1 are mandatory unless marked optional.

C.2.8.5.4.1 Managed Security Service Performance Metrics

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Availability (Port) for TICS	Routine	99.95%	≥ 99.95%	See Note 1
	Critical	99.995%	≥ 99.995%	
Latency (CONUS) for TICS	Routine	60 ms	≤ 60 ms	See Note 2
	Critical	50 ms	≤ 50 ms	
GOS (Data Delivery Rate) for TICS	Routine	99.95%	≥ 99.95%	See Note 3
	Critical	99.995%	≥ 99.995%	

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Event Notification (EN) Security Incident Reporting for TICS	Routine	Near real time	≤ 30 min	See Note 4
Event Notification (EN) for MPS	Routine	Within 10 minutes	≤ 10 minutes	
Event Notification (EN) for INRS	Routine	Next business day or within 24 hours for a Low category event	≤ Next business day or 24 hours	See Note 5
		Within 4 hours of a Medium category event	≤ 4 hours	
		Within 1 hour of a High category event	≤ 1 hour	
Grade of Service (Configuration Change, Virus Protection Updates)	Routine	Within 5 hours (for MPS) and 24 hours (for VSS) for a Normal priority change	≤ 5 hours (MPS) and ≤ 24 hours (VSS)	See Note 6
		Within 2 hours for an Urgent priority change	≤ 2 hours	
Incident Response Time (Telephone)	Routine	Within 1 hour of the notification for a Low category incident	≤ 1 hour	See Note 7
		Within 15 minutes of the notification for a High category incident	≤ 15 minutes	
Incident Response Time (On-Site)	Routine	Within 36 hours of the notification for a Low category incident	≤ 36 hours	See Note 8
		Within 24 hours of the notification for a High category incident	≤ 24 hours	
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 9

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. MSS availability is calculated as a percentage of the total reporting interval time that the MSS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. TICS Port availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the port is operationally available to the agency. The TICS Port availability metric does not apply for DSL and Cable High Speed (i.e. BIS) access methods. Availability is computed by the standard formula:

$$Av(Port) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

3. Latency is the average one-way time for IP packets to travel over the EIS core network. The Backbone Latency metric does not apply for DSL and Cable High Speed (i.e. BIS) access methods.
4. Security incident reporting to the CISA Incident Reporting System must be performed in near real-time, congruent with NIST SP 800-61 Rev 2, not to exceed 30 minutes, from the time of confirmed incident detection.
5. The Event Notification (EN) value represents the elapsed time between the detection of the event and the notification of the agency. Events are categorized as follows:
   a) Low — Events in the Low category have a negligible impact on service. They include firewall incidents that do not significantly affect network security, as well as minor hardware, software and configuration problems.
   b) Medium — Events in the Medium category have a more serious impact on service, and may indicate a possible security breach, threat or attack attempt. They may also cause the service to operate in a degraded state.
   c) High — Events in the High category represent firewall violations that severely impact service and operations. They indicate a true compromise of network

security. These events also include major hardware, software and configuration problems, and are immediately reported via email or telephone, as specified by the agency.

6. The Grade of Service (Configuration Change) value represents the elapsed time between the configuration change request and the change completion. Changes are initiated and prioritized by the agency, or may be implemented in response to an event. Changes initiated by the contractor require agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency). Exceptions may be associated with agency-specified and agreed-upon maintenance windows that require pre-planned integration.
7. The Telephone Incident Response value represents the elapsed time between the agency's notification to the contractor and the contractor's implementation of response procedures. These procedures, and what constitutes Low and High incidents, are defined in the TO.
8. The On-Site Incident Response value represents the elapsed time between the agency's notification to the contractor and the contractor's arrival to the affected site for implementation of response and investigative procedures. These procedures, and what constitutes Low and High incidents, are defined in the TO.
9. Time to Restore (TTR) for MSS solutions leveraging the Broadband Internet Service (BIS) will default to the BIS TTR Performance Metrics in Section C.2.1.8.4 for the components leveraging BIS.

C.2.8.6 Managed Mobility Service

C.2.8.6.1 Service Description

Managed Mobility Service (MMS) helps agencies manage the transition to a more complex mobile computing and communications environment by supporting security, network services, and software and hardware management for mobile handheld devices. This is especially important as Bring Your Own Device (BYOD) initiatives and advanced wireless computing become the focus of many agencies.

MMS is a core capability for effectively scaling the secure deployment and management of mobile applications, enterprise data on mobile devices, and management of the devices and mobile platforms themselves. The optimal balance between security, total costs and functionality will provide the most business value to the agencies.

MMS may be offered as a cloud-based, premises-based, or hybrid solution.

C.2.8.6.1.1 Functional Definition

MMS supports mobile computing by allowing agency-owned and personal mobile handheld devices (smartphones and tablets, based on smartphone OSs) to access agency networks and applications in accordance with the agency's IT security policy. MMS supports mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), mobile security, deployment support, and Mobility-as-a-Service (MaaS).

C.2.8.6.1.2 Standards

MMS shall comply with the following standards:

1. FISMA Moderate Impact level or higher
2. NIST SP 800-53 Moderate
3. FIPS 140-2/3
4. IPv4 and IPv6
5. The specific standards, as identified in the TO

C.2.8.6.1.3 Connectivity

MMS shall interoperate with:

1. 3G/4G/5G and future evolutions of Cellular Service, based on standards for CDMA, GSM, LTE, and NR
2. Laptops, Smartphones, Tablets, and other mobile devices
3. Wi-Fi

C.2.8.6.1.4 Technical Capabilities

MMS capabilities are subdivided into MDM, MAM, MCM, Mobile Security, Deployment Support, and MaaS which are described in the following subsections.

C.2.8.6.1.4.1 Mobile Device Management (MDM)

MDM supports device management and other mobile management functions including operations, policy, security, configuration, mobile network performance, application support (application performance, version control, distribution, etc.), mobile data management (on device), and some mobile network monitoring.

The following capabilities are mandatory unless marked optional:

1. MDM capabilities include, but are not limited to, the following:
   a) Enforce enterprise rules while allowing agency/bureau/sub-bureau/etc. enrollment, reporting, management, and compliance activities.

b) Take the following action upon a group of devices from a search: Reassign to Group (any type of logical grouping, e.g., user or device groupings).

c) Assign Profile to one or many Groups (any type of logical grouping). User or device groupings are an example.

d) View required applications from a Mobile Application Store (MAS).

e) View and run reports on user and device information for all Smartphones including usage and cost.

f) Run reports by groups of users to include location.

g) Support a Software Development Kit (SDK) or API Framework to integrate with existing or future agency applications.

h) Monitor the MDM system via industry standard tools.

i) Integrate certificates from the MDM system's internal PKI system to mobile devices as well as third party public PKI providers.

j) Perform MDM functions from within a secure VPN used to transport all enterprise/agency data (i.e.: no MDM control data is transported unencrypted across the open Internet).

2. Device Enrollment – adding a device to the MDM management domain:

a) Set a Target Platform (Apple, Android, Microsoft Windows, etc.) for profile provisioning.

b) Use a Target Device Model for profile provisioning.

c) Specify minimum OS version for profile provisioning.

d) Use Target Device Ownership (GFP, personal, etc.) for profile provisioning.

e) Allow a user to edit any field for a "live" or "active" profile.

f) Allow a user with appropriate authorization to self-enroll an agency GFP or BYOD device.

g) Centrally manage multiple devices for a single user (user device view).

h) Support different policies or grouping for multiple devices under one user (i.e.: tablet policy, smartphone policy).

i) Apply multiple policies to devices simultaneously (user is member of group policy X, with device policy Y) – when multiple controls conflict, the most restrictive control takes precedence.

j) Use external directory service repository for enrollment.

k) Use federated (i.e., SAML, OAuth, etc.) and multi-factor authentication for enrollment and restrict enrollment based on directory-based security groups

l) Set support email and phone information for registration messages.

m) Redirect users to a URL upon successful enrollment.

n) Edit an enrollment activation notification message to the user (email and/or SMS).

o) Set a default Device Ownership type upon enrollment for different groups.

p) Use an internal user list for enrollment for different groups.

q) Set support email and phone information for registration messages for different groups.

r) Edit an enrollment activation notification message to the user or group of users (email and/or SMS).

s) Send a user or group an activation enrollment message (email or SMS).

3. Device Profiles (per-user and per-group):

a) Create a profile template.

b) Copy profiles.

c) Edit a "live" or "active" profile.

d) Set Profile Removal Permission (who can remove a profile from a device or user).

e) Set Profile Start Date (when the profile starts applying to associated devices).

f) Set Profile End Date (when the profile stops applying to associated devices).

g) Automatically update a device that currently has a profile when editing that profile, and set Profile Geofences (profiles are active/inactive depending on physical device location).

h) Push a profile to any individual device.

i) Automatically remove profiles from devices whose state changes from qualifying to not-qualifying. This may happen as a result of changing a profile to be more exclusive.

j) Support multiple profiles being applied to a single device (most restrictive rules apply).

k) Delete a profile from the MDM system.

l) Set a description for a profile.

m) Manage the following via a profile:

i. Install applications
ii. Control use of camera
iii. Control use of installed applications, including default applications
iv. Allow multiple Wi-Fi configurations for multiple profiles
v. Manage device Wi-Fi settings via a MDM policy

vi. Control Wi-Fi Security Type: None, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA/WPA2), Enterprise/agency-specific (any)
vii. Multiple VPN configurations for a single profile
viii. VPN Connection (or Policy) Type: IPSec and TLS
ix. VPN connection Proxy for a VPN configuration
x. Multiple email/calendar/contact configurations per profile
xi. Multiple Web Clip / Web Shortcut configurations per profile

4. Device Feature Management:

a) Multi-OS Support – Manage multiple OS devices.

b) Device passcode enforcement (complexity, length, presence).

c) Installation of applications (See MAM)

d) Camera (enable/disable).

e) Control radios/communications:

i. Wi-Fi (enable/disable)

ii. Bluetooth (enable/disable)

iii. Enable or disable specific hardware component and uses, such as enable Bluetooth headphone, disable Bluetooth keyboard

iv. Near Field Communication (NFC) (enable/disable)

v. GPS (enable/disable)

vi. Store enterprise/agency data to removable media (disable)

5. Data Management – read, write, transmit and receive data on mobile devices as well as with backend systems/repositories:

a) File Management – to secure data, files, and applications (e.g., pdf files or Word docs) on a mobile device

b) Personal Information Management – mail, calendar, and address book capabilities

6. NIST SP 800-126 Security Content Automation Protocol (SCAP) support for the server-side components, including asset management, configuration management, patch management and remediation capabilities.

7. Device Inventory Management and Reports – to provision, control and track devices connected to corporate/agency applications and data, and to relate this data to user information, in accordance with the TO. Device Inventory Reports include all data associated with the device, OS and applications.

8. System Performance Reports – include key performance data to provide insight into the reliability of the solution, and device usage and performance, in accordance with the TO.
9. MDM Security/Compliance Reports – Security reports include all data relevant to the monitoring and support of the system's vulnerabilities and defenses, including attempts at fraud in accordance with the TO. Security status reports shall be run as requested.
10. The following capabilities may be defined at the TO level:
    a) (Optional) Quality of Service (QoS) – shall support QoS capabilities to prioritize real-time or latency-sensitive application data where appropriate (e.g.: VoIP, video, real-time chat). It shall be possible to enforce and exclude QoS priority by application or protocol to prevent non-real-time applications from inappropriately increasing their traffic priority.
    b) (Optional) Classified Data – shall support access classified data up to the SECRET level via mobile devices.
    c) (Optional) PIV/CAC Support – shall support the management of PIV/CAC cards and/or derived credentials on mobile devices via the MDM.
    d) (Optional) Biometric Support – shall support biometric support such as fingerprint or face recognition with mobile devices. The ability for the MDM to manage this capability may be combined with PIV / CAC support.
    e) (Optional) Network Monitoring – shall support monitoring of the mobile device network quality and performance (e.g., the number and location of dropped calls by enterprise/agency devices).

C.2.8.6.1.4.2 Mobile Application Management (MAM)

The following capabilities are mandatory unless marked optional:

1. Application Deployment:
    a) Commercial Application Store (enable/disable)
    b) Reporting of installed applications
    c) Block application purchase
    d) Application Whitelisting/Blacklisting
    e) Staged/controlled application deployment (limit deployment by policy, group, location, etc. to facilitate gradual deployment of new or updated applications)
2. Mobile Application Store (MAS):
    a) MAS shall allow users to select private enterprise/agency applications for installation on managed devices. This capability shall be integrated into the

MDM portal and shall allow application provisioning by group policy and mandatory application deployment. MAS shall support the following capabilities:

i. Add/update an application from a Commercial Application Store to the MAS
ii. Add/update an enterprise/agency application to the MAS via a web GUI
iii. Add additional metadata to and report on metadata on any application added to the MAS (name, description, version, OS, keywords, etc.)
iv. Specify the effective date for an agency internal application
v. Specify the expiration date for an agency internal application
vi. Specify the minimum operating system and model for an agency internal application
vii. Download agency internal and public applications from MAS
viii. Categorize, group or tag applications (e.g., business applications, scientific applications, etc.)

3. Application Security:

a) Mutual Authentication – MDM applications on the device and services must mutually authenticate using certificate-based authentication to ensure the communications channel is not intercepted.

b) Application Installation Control – shall support relevant authorizations and approvals (include change tracking) to control downloading of authorized and unauthorized applications and help ensure user compliance. This includes the ability to monitor application usage.

c) Blacklisting / Whitelisting –block and/or remove specified applications (Blacklisting), and permit or force the installation of specified applications (Whitelisting).

d) Application Environment Requirements – detect and enforce device environment conditions such as:

i. Minimum or specific operating system versions
ii. Required presence or absence of other applications
iii. Absence of privilege escalation (“rooting” or “jailbreaking”)

e) Application Signing – shall support requiring digital signatures for application installation, from both commercial and private application stores and direct application push / deployment.

4. The following capabilities may be defined at the TO level:

a) (Optional) Third-party Application Mutual Authentication to provide third-party applications with mutual authentication and secure communications through wrappers, binary patching, etc.

b) (Optional) MAM Software Integration Services to support the delivery of new or existing enterprise/agency applications to mobile devices, such as data entry system accessible to field workers.

C.2.8.6.1.4.3 Mobile Content Management (MCM)

MCM enables secure mobile access to content anytime, anywhere, and on any device. It protects sensitive content and provides users with a central application to securely access, store, update and distribute documents.

C.2.8.6.1.4.4 Mobile Security

The following capabilities are mandatory unless marked optional:

1. Enroll a device before applying any policy (null policy)
2. Create Whitelists/Blacklists for device enrollment to include OS versions and device models
3. Allow enrollment of untrusted devices and anonymous / unknown users outside the enterprise as individuals or to groups under the MDM
4. Use an existing MDM user attribute repository for enrollment to the new MDM system
5. Take action based on compliance rules, in support of MDM's ability with active (device scanning) and passive (on-access scanning) tools to detect, report, and alert on a compromised device (e.g.: jail broken / rooted device, malware)
6. Block the device or to erase (wipe) only the managed data on a device under the following conditions:
   a) Blacklisted operating system or version (policy based)
   b) Exceeding a set number of failed access attempts to the device or MDM application (policy based)
   c) Exceeding defined interval for contacting MDM (policy based)
   d) Detection of OS jailbreaking or application tampering (policy based)
   e) Any other policy violation
   f) Remote instruction from MDM (manual)
7. Password policy enforcement:
   a) Minimum complexity (length, composition, common words, etc.)
   b) Password lifetime limit
   c) Password re-use limits

   d) Password inactivity timeout (grace period) for device and MDM application
   e) Report password failures beyond threshold to MDM
   f) Maximum password attempts before lock or wipe
8. Mask passwords when they appear in the Management GUI
9. Determine which administrative user made a configuration change in the MDM administrative environment
10. Determine which device user made a configuration change in the MDM console (self-service logging)
11. Installation and configuration (update, revocation checking, revocation) of individual and group soft authentication certificates for the following purposes:
    a) Email (S/MIME) signing and encryption
    b) Wi-Fi Configuration
    c) VPN Configuration
12. Send/receive (encrypt and sign, decrypt and verify) messages that use PKI or S/MIME encryption, where email functionality is delivered by the service/system
13. Restrict downloading attachments, copying of data to/from removable media, or otherwise create separate spaces or virtual containers for agency data and applications from personal data
14. (Optional) View the current GPS location of a device or logical grouping of devices on a map
15. Encrypt the data in transit between the MDM and the device in accordance with FIPS 140-2/3
16. The data at rest on a mobile device shall be separated in different containers for agency data and personal data, and shall protect agency data from access by uncontrolled applications to limit interaction between agency data and personal data. The agency data shall be encrypted if the underlying platform does not encrypt all data on the device.
17. User Authentication shall support PIN or password authentication for the managed applications, and optionally multifactor authentication with any two of the following three authentication types:
    a) Shared Secret – something the user knows, like a PIN or password
    b) Token – something a user possesses such as a cryptographic key such as an RSA token (soft or hard), a challenge/response token, a PIV or CAC, or a key generator device
    c) Biometric – a sufficiently unique physical characteristic of the user, such as a fingerprint, iris or facial image

18. User Compliance:
    a) Set up compliance rules to include custom compliance rules for profiles, devices, groups, and Whitelist/Blacklist
    b) Activate/deactivate a compliance rule
    c) Specify user and group rules for application compliance, such as required or prohibited applications on a device
    d) Provide enterprise level compliance reports, including lost/wiped/inactive devices, the total number of devices, the number of devices active, how much data is sent/received by devices, and connection type
19. Alerting – notify agency operations staff about agency devices:
    a) Set up custom alerts to users and management based upon various parameters
    b) Send custom alerts to one or more user roles including administrators
    c) Specify a creation policy for custom alerts to include having various alert severity levels
    d) Create automated alerts for security issues such as compromised devices
    e) Create alerts based upon device status such as battery low, device roaming, equipment down (not responding), device inactive, etc.
    f) View alerts pending acknowledgement
    g) Acknowledge alerts and track acknowledgements
20. Audit reports – provide data necessary to monitor, reconcile, and audit system processing and reconciliation activities. Audit reports shall be exportable, and shall be run as requested by the agency.
    a) Administrator activity (actions performed, time stamps, etc.)
    b) User access times and enrollments
    c) Devices (number of devices by agency and across all sub-agencies, type, OS version, etc.)
    d) Console logins and functions (connections to the management console, actions performed, etc.)
    e) Policy changes and versions (policy revision control and historical changes)
    f) Policy violations
21. Safeguard any Personally Identifiable Information (PII), including directory data stored in the information system in accordance with NIST SP 800-122.

C.2.8.6.1.4.5 Deployment Support

The following capabilities are mandatory unless marked optional:

1. Deployment:
    a) The contractor shall support MMS for installing, configuring, and certifying the initial deployment of the MDM, MAM and Container solutions, as well as the ability to support specific agency- related integrations or customizations, as specified in the TO. The contractor shall assist the agency with achieving accreditation and authorization (compliance) objectives by producing supporting documentation and/or modifications to the solution to reach compliance.
2. Enterprise Systems Integration:
    a) The contractor shall assist in deploying and integrating its MMS into the agency-wide environment. This includes systems such as enterprise email, directories, trouble-ticketing, etc.
3. Training:
    a) The contractor shall provide MDM/MAM training material content, as well as providing pre-packaged online training and associated materials in accordance with the TO.
4. Help Desk:
    a) The contractor shall provide a Help Desk for MDM/MAM that supports online requests / resolutions via email and telephone.

C.2.8.6.1.4.6 Mobility-as-a-Service (MaaS)

Mobility-as-a-Service (MaaS) is a subscription-based service enabling mobile endpoints to be delivered and securely managed as a consumable service. In this context a mobile endpoint is a user interface that requires wireless connectivity to communicate with an enterprise or carrier network. The service provider retains asset ownership of the endpoint(s) and provides services regarding asset issuance, endpoint performance management, service plan management, the mobility management software, and customer support services into a full solution that minimizes prior device-centric costs and operations. Under MaaS, third-party mobility providers are responsible for the mobility of your organization, from device staging and kitting, to replacement and protection, to managing cross-carrier wireless access and pooling. MaaS includes end-to-end service delivery and management with respect to:

- Planning and management of agency MaaS needs and solutions
- Provisioning, kitting, and service delivery
- Enterprise Mobility Management (EMM) or Unified Endpoint Management (UEM)
- Ongoing customer support
- Logistics for device refresh and end-of-life disposal/recycling

The following capabilities are mandatory unless marked optional:

1. Solutions shall ahere to the EIS Wireless Service (MWS) Standards, Technical Capabilities and Features in Section C.2.6 for the underlying wireless services proposed as part of the MaaS.
2. Solutions shall meet or exceed the EIS MMS Section C.2.8.6.1.4 Technical Capabilities within the MDM, MAM, MCM, Mobile Security, and Deployment Support subsections.
    a. Based on agency requirements, contractors may propose additional MMS Features listed in Section 2.8.6.2 to supplement and enhance their MaaS offerings.
3. The contractor shall implement mobile device management, mobile application management, mobile identity management/integration, mobile content management, and data containerization (separating corporate and personal data).
4. The contractor shall manage device issuance to and retrieval from end users. This support shall include staging and kitting, depot repair, advanced replacement, recycling, and device refresh in accordance with Section C.2.6 of the EIS contract.
5. The contractor shall implement and manage secure access to corporate resources and content through authentication, encryption, containerization, and enterprise file synchronization and sharing (EFSS) capabilities.
6. Sourcing management leveraged to purchase, provision and activate network services, applications, and devices.
7. Financial management capabilities which include sourcing, ordering, provisioning, inventory, usage, and invoice management and reporting.
8. The contractor shall provide program management services to manage the MaaS capabilities, service requests, account(s), and third-party providers the contractor may leverage to deliver their solution.

C.2.8.6.2 Features

The MMS features are mandatory unless marked optional.

ID Number	Name of Feature	Description
1 (Optional)	Mobile Threat Protection (MTP)	Mobile Threat Protection (MTP) is a component of a layered Mobile Endpoint Protection Strategy that covers the major areas not addressed by the MDM, MAM, MCM or Mobile Security technical capabilities. MTP solutions monitor the mobile device in real-time to identify mobile threats that may compromise the device, mobile applications, or data residing on the device. MTP integrates with a MDM system deployed on devices resulting in remediation or quarantining of the threat. The MTP solution evaluates an application threat and compliance against a set of pre-defined agency policies based upon acceptable risks, it validates operating system (OS) integrity against any compromise, it detects network threats such as MITM (Man-in-the-Middle) attacks and will detect device configuration risks.
2 (Optional)	Mobile Application Vetting	Mobile Application Vetting (also referred to as app threat intelligence or threat protection services) refers to software, processes, and tools required to test, validate, and verify mobile apps against a baseline of security, privacy, and organization-specific requirements and policies. Vendors may provide on premise, cloud-based, or outsourced app vetting solutions that run static and/or dynamic analysis tests and reporting on apps to detect security vulnerabilities and malicious or privacy violating behaviors.

ID Number	Name of Feature	Description
3 (Optional)	Mobile Identity Management	Mobile Identity Management is the secure integration of the attributes that unerringly identify a person in the physical and online environments, within the mobile device. MIM is a set of complementary products and solutions that issue and maintain certificates, which may include Derived PIV Credential (DPC) usage. Once issued, credentials on a mobile device will support: • Wi-Fi authentication • Virtual Private Networking • User authentication to Commercial off the Shelf (COTS), Software-as-a-Service (SaaS), and other applications and services • Data in Transit • Data Encryption • Signing of individual documents and records
4 (Optional)	Mobile Backend-as-a-Service (MBaaS)	MBaaS represents mobile application delivery solutions that provide mobile application developers with a platform, tools, and libraries to develop, integrate, test and publish their applications to backend cloud storage and processing resources while also providing common features such as user management, push notifications, social networking integration, and other features demanded by mobile users.

ID Number	Name of Feature	Description
5 (Optional)	Internet of Things (IoT)	Internet of Things (IoT) service providers engage with those who design, develop, operate, secure, or maintain an infrastructure of networked components comprised of computing resources, digital sensors, actuators, and human interfaces that are combined into systems to achieve specific goal(s).

C.2.8.6.3 Interfaces

The MMS shall support the UNIs for all Smartphones and Tablets (based on smartphone OSs) operating under 3G/4G/5G and future evolutions of Cellular Service (based on standards for CDMA, GSM, LTE, and NR) as required.

C.2.8.6.4 Performance Metrics

The MMS performance levels and AQL of KPIs in Section C.2.8.6.4.1 are mandatory unless marked optional.

C.2.8.6.4.1 Managed Mobility Service Performance Metrics

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Event Notification (EN)	Routine	Next business day or within 24 hours for a Low category event	≤ Next business day or 24 hours	See Note 1
		Within 4 hours of a Medium category event	≤ 4 hours	
		Within 30 minutes of a High category event	≤ 30 minutes	
Grade of Service (Configuration Change)	Routine	Within 5 hours for a Normal priority change	≤ 5 hours	See Note 2
		Within 2 hours for an Urgent priority change	≤ 2 hours	

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Telephone Incident Response Time	Routine	Within 1 hour of the notification for a Low category incident	≤ 1 hour	See Note 3
		Within 15 minutes of the notification for a High category incident	≤ 15 minutes	
Dispatch Incident Response Time	Routine	Within 36 hours of the notification for a Low category incident	≤ 36 hours	See Note 4
		Within 24 hours of the notification for a High category incident	≤ 24 hours	
Availability	Routine	99.5%	≥ 99.5%	See Notes 5 and 6
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. The Event Notification (EN) value represents the elapsed time between the detection of the event and the notification of the agency. Events are categorized as follows:

    a) Low — Events in the Low category have a negligible impact on service. They include firewall incidents that do not significantly affect network security, as well as minor hardware, software and configuration problems.

    b) Medium — Events in the Medium category have a more serious impact on service, and may indicate a possible security breach, threat or attack attempt. They may also cause the service to operate in a degraded state.

    c) High — Events in the High category represent firewall violations that severely impact service and operations. They indicate a true compromise of network security. These events also include major hardware, software and configuration problems, and are immediately reported via email or telephone, as specified by the agency.

2. The Grade of Service (Configuration Change) value represents the elapsed time between the configuration change request and the change completion. Changes are initiated and prioritized by the agency, or may be implemented in response to an event. Changes initiated by the contractor require agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency).
3. The Telephone Incident Response value represents the elapsed time between the agency's notification to the contractor, and the contractor's implementation of response procedures. These procedures, as well as what constitutes Low and High incidents, are defined in the TO.
4. The Dispatch Incident Response value represents the elapsed time between the agency's notification to the contractor, and the contractor's arrival to the affected site for implementation of response and investigative procedures. These procedures, as well as what constitutes Low and High incidents, are defined in the TO.
5. MMS availability is calculated as a percentage of the total reporting interval time that MMS is operationally available to the agency. Availability is computed by the standard formula: $Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$
6. MMS MaaS radio access network performance is likely to vary depending on location (e.g., urban, suburban, or rural), as well as the technical specifications and capabilities of the deployed infrastructure, such as the radio access equipment.

C.2.8.7 Audio Conferencing Service

C.2.8.7.1 Service Description

The government has a large community of audio conferencing users. The following sections provide the requirements for Audio Conferencing Service (ACS).

C.2.8.7.1.1 Functional Definition

ACS enables participants to engage in a multi-point audio conference call. The audio connection from the conference participants to the ACS conference-bridge is provided by voice service (IPVS, CSVS) and cellular voice service.

C.2.8.7.1.2 Standards

ACS shall comply with the following standards:

1. ANSI T1.101 for T1

2. ANSI T1.607 and 610 for ISDN
3. ANSI SS7, and enhanced SS7 standards for interworking (e.g., address translation) between circuit-switched network and IP network
4. Telcordia Notes on the Networks (SR-TSV-2275)
5. IETF RFC 3661 through 3665 for SIP (Session Initiation Protocol)
6. IETF RFC 3435 for MGCP (Media Control Gateway Protocol)
7. ITU-TSS H.323/225/245/248 (enhanced for VoIP)

The contractor shall comply with new versions, amendments, and modifications made to the standards listed above.

C.2.8.7.1.3 Connectivity

ACS shall connect to and interoperate with:

1. Customer-specified locations
2. PSTN
3. Internet
4. The contractor's network and all other contractors' networks for CSVS and IPVS

C.2.8.7.1.4 Technical Capabilities

The following ACS capabilities are mandatory unless marked optional:

1. Multi-point Bridging Capability. Support selective two-way or one-way conversations between conferencing ports (i.e., allow a subset of conferees to participate in a two-way conference while the remaining conferees are listeners only). During a multi-point conference, the addition of a party to, or the deletion of a party from, the conference shall be indicated by a tone or verbal announcement.
2. Conference Set-up Capability. Provide the following conference set-up support services:
    a) User-Controlled Conference. Allow authorized users and users with a calling-card to establish a conference call by dialing a designated number to access the service. The following two automated modes of user-initiated conferencing capabilities shall be supported:
        i. Meet-Me Conference – Allow each user to be connected in a conference by dialing a designated number and authorization/pass code at a predetermined time or as directed by the operator. For recurring meet-me conferences, the contractor shall permit the participants to reuse the same dial access number and authorization/pass code and allow bookings of recurring conferences.

   ii. Preset Conference – Allow an authorized user to activate a previously-defined conference with associated conferees by dialing an access number followed by an authorization/pass code. Once activated, the system shall attempt to connect the pre-designated participants using the predefined lists.

  b) Attendant-Assisted Conference. Allow operators to establish a conference. Conferees shall be able to call an operator during a conference for immediate attention, such as general assistance or adding or dropping participants.

3. Audio Conference Reservation System.
4. Automatic port expansion. Support, without operator assistance, automatic expansion to support additional users to the conference in progress beyond the dial-in ports reserved as long as facilities are available.
5. Conferee tones. Enable or disable conferee tone when a participant enters or exit a conference.
6. Participant count.
7. Roll call.
8. Attendant assistance. Available at any time during an audio conference.

C.2.8.7.2 Features

The following ACS features are mandatory unless marked optional.

1. Audio recording of call. Allow recording of conference call into storage media for later replay.
2. Spanish language translation. Provide language translation to English from Spanish for transcription of a pre-recorded audio conference.
3. (Optional) Language translation. Provide language translation to English from languages other than Spanish for transcription of a pre-recorded audio conference.
4. Moderator-led Q&A.
5. Participant list report.
6. Password-protected session.
7. Download and replay a pre-recorded audio conference.
8. Transcription of audio call.
9. Temporary blocking. Allow temporary blocking of audio conference participants in order to remove a sub-set of participants/users from the conference.

10. (Optional) Secured Audio Conference. Support sensitive voice conferences with end-user encryption for discussions of a CUI nature between multiple locations with protection from unauthorized interception (i.e., eavesdropping).
11. Operator dial-out. The capability to add a participant to a conference via an outbound call from the conference bridge initiated by the conference attendant.
12. Host dial-out. The capability to add a participant to a conference via an outbound call from the conference bridge initiated by the conference host.
13. Executive conference. Conference requires professional moderator assistance with control of conference attendant functions.
14. International global meet. The feature provides in-country local access which is a non-North American toll number assigned to a specific country and bridge.
15. Host controls. The conference host has the capability to control conference attendant functions.

C.2.8.7.3 Interfaces

The contractor shall support audio connection to the conference bridge from services such as voice service (e.g., CSVS and IPVS), and cellular voice service.

C.2.8.7.4 Performance Metrics

The ACS performance levels and AQL of KPIs are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
GOS (Operator Assistance Response Delay)	Routine	30 seconds	≤ 30 seconds	See Note 2
Time to Restore	With Dispatch	8 hours	≤ 8 hours	
	Without Dispatch	4 hours	≤ 4 hours	

Notes:

1. ACS availability is calculated as a percentage of the total reporting interval time that ACS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. GOS (Operator Assistance Response Delay) is the delay experienced by conference participants to receive operator assistance during a conference. Delay is measured as the interval between the end of signaling (e.g., dialing for operator assistance) and the receipt of voice response from the operator.

C.2.8.8 Video Teleconferencing Service

C.2.8.8.1 Service Description

Video Teleconferencing Service (VTS) enables participants at different locations to simulate face-to-face meetings and conduct interactive dialogue with instant sharing of various applications and documents.

C.2.8.8.1.1 Functional Definition

VTS will offer point-to-point and multi-point conferencing with audio conference add-on capabilities to support the following three user configurations: 1) desktop, 2) portable roll about, and 3) fixed conference room locations.

C.2.8.8.1.2 Standards

VTS shall comply with the following standards:

1. Federal Telecommunications Recommendations (FTR) 1080B - 2002 (hereinafter referred to as FTR-1080) issued by the Technology and Standards Division of the National Communication System (NCS).
2. FTR 1080 encompasses the specifications for narrow-band audio and video teleconferencing, from 56 Kbps to 1920 Kbps, primarily based on the following standards:
    a) ITU-T H.320 recommendations for telephony networks
    b) ITU-T H.323 recommendations for packet based multi-media conferencing
    c) ITU-T H.239 for H.320 for document conferencing
3. IETF RFC 3261 Session Initiation Protocol (SIP).

The contractor shall comply with new versions, amendments, and modifications made to the documents and standards listed above.

C.2.8.8.1.3 Connectivity

VTS shall connect to and interoperate with:

1. IP Networks
2. PSTN

C.2.8.8.1.4 Technical Capabilities

The following VTS capabilities are mandatory unless marked optional:

1. Allow participants at different physical locations to simulate in-person meetings and conduct interactive dialogue using point-to-point and point-to-multi-point video teleconferencing arrangements.
2. Support two-way video, one-way video with interactive voice, and/or the instant sharing of various types of documents/data files among VTS participants as an adjunct to the video teleconferencing session.
3. Support document sharing (data conferencing) which enables conference participants to interactively view, edit, and share or transfer data files and documents.
4. Provide an audio conference add-on capability to support non-video conference participants in a VTS call.
5. Provide teleconferencing bridge capabilities.
6. Support the following modes of operation:
    a) Dial-Out mode: A centralized arrangement where the conference bridge operator initiates a call and dials each participant
    b) Meet Me (Dial-In) mode: Each participant is responsible for individually initiating a call and dialing into the conference bridge.
    c) Mixed Dial mode: Support a combination of both dial-out and meet me (dial-in) callers
7. Provide the capability for VTS users to request operator assistance to resolve technical issues.
8. Maintain synchronization between the audio and video signals.
9. Allow users to establish a point-to-point VTS on demand without a reservation. Point-to-point VTS shall include full-duplex video, audio, and ancillary data transmission between participating locations.
10. Provide VTS multi-point arrangements in conjunction with the contractor’s VTS reservation system. The multi-point arrangement shall have the capability of simultaneously providing VTS to users of a different EIS contractor’s network and to users of public or other private networks. During a multi-point conference, the

addition of a party to, or the deletion of a party from, the conference shall be indicated by a tone or by a verbal or visual announcement.

11. Provide access to a secure central reservation system to permit authorized VTS users to schedule multi-point video teleconferences.
12. Provide a video format conversion capability that permits operation between the following:
    a) CODECs which operate in the NTSC video format and CODECs which operate in the Phase Alternation by Line (PAL) video format.
    b) CODECs which operate in the NTSC video format and CODECs which operate in the Système Electronique Couleur Avec Memoire (SECAM) video format.
13. Traverse and successfully interoperate with agency firewalls and security layers. The contractor shall verify with the agency that the agency firewall is compatible with this service.
14. Provide VTS reports in accordance with the TO.

C.2.8.8.2 Features

The following VTS features are mandatory unless marked optional:

1. Attended Service: The contractor shall provide call monitoring, roll call, and coordination for a VTS conference.

2. Verification: The contractor shall provide pre-testing, registration, and verification that agency-owned equipment operates correctly with the contractor’s VTS.

3. Coding Conversion (Transcoding):

    a) Provide transcoding that is compliant with FTR 1080 formats.
    b) (Optional) Provide a coding conversion capability that permits operation between CODECs, all of which use the National Television Standards Committee (NTSC) video format, but none of which support the FTR 1080 standard and none of which use the same encoding/decoding algorithm(s). At a minimum, the contractor shall support the following compression algorithms as needed by the agency: SG3/SG4, CTX, and CTX+.
    c) (Optional) Provide a coding conversion capability that permits operation between CODECs, all of which use the NTSC video format, in which one or more of the CODECs support the FTR 1080 and in which one or more of the CODECs do not support the FTR 1080. At a minimum, the contractor shall support the following compression algorithms as needed by the agency: SG3/SG4, CTX, and CTX+.

4. (Optional) Rate Adaptation: Provide a data rate adaptation capability to ensure that all VTS locations participating in a video teleconference can interconnect with each other at dissimilar data rates.
5. (Optional) Security – CUI: Provide transparent and secure VTS communications paths to support CUI video communications. The security capabilities are described in the FTR1080 recommendation.
6. (Optional) Security – Classified: Provide transparent and secure VTS communications paths and support video information that is categorized as classified (National Security agency type 1 encryption) video communications. The security capabilities are described in the FTR1080 recommendation.

C.2.8.8.3 Interfaces

The VTS UNIs at the SDP as defined in Section C.2.8.8.3.1 are mandatory unless marked optional.

C.2.8.8.3.1 Video Teleconferencing Service Interfaces

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	Digital Trunk: T1 (Std: Telcordia SR-TSV-002275 and ANSI T1.102/107/403)	Up to 1.536 Mbps	T1 Robbed-Bit Signaling
2	Digital Trunk: ISDN PRI T Reference Point (Std: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931
3 (Non-Domestic / OCONUS)	Digital Trunk: E-1 Channelized (Std: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling
4	All IEEE 802.3 cable and connector types	Up to 100 Mbps	IEEE 802.3. IPv4 and IPv6

1. If the agency provides the CODEC and the inverse multiplexer, and the contractor provides only reservation, coding conversion, and/or format conversion, the UNIs supported shall include:
   a) ITU-TSS V.35

b) EIA RS-449

c) EIA RS-530

d) RJ-x (e.g., RJ-45)

e) Data Interface(s) – the VTS shall support any combination of the following:

   i. EIA RS-232

   ii. EIA RS 449

   iii. ITU-TSS V.35

   iv. EIA RS-530

C.2.8.8.4 Performance Metrics

The VTS performance levels and AQL of KPIs in Section C.2.8.8.4.1 are mandatory unless marked optional.

C.2.8.8.4.1 Video Teleconferencing Service Performance Metrics

KPI	User Type	Performance Standard (Threshold)	AQL	How Measured
Availability	Routine	99.5%	≥ 99.5%	See Note 1
Grade of Service (Completed Service Requests)	Routine	95% of VTS conference requests met	≥ 95%	See Note 2
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. Availability is measured and calculated as a percentage of the total reporting interval time that VTS is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

2. The Grade of Service (completed service requests) applies to video conferences that are reserved and confirmed. It shall be calculated as the ratio of the number of locations successfully completing a VTS call divided by the total number of locations scheduling a VTS call within a calendar month. Locations that schedule a video conference and then decide not to join will be treated as successfully completing a VTS call for Grade of Service (Completed Service Requests). The contractor shall compute the number of completed service requests by counting the cumulative number of locations associated with each conference that were successfully completed. The contractor shall compute the number of service requests denied by counting the cumulative number of locations associated with each VTS conference that could not be scheduled for a particular date and time requested in a calendar month. VTS calls that were disconnected and then re-established only due to the fault of the contractor would be included as a denied request.

C.2.8.9 DHS Intrusion Prevention Security Service (DHS Only)

The Intrusion Prevention Security Service (IPSS) consists of the use of classified and unclassified Government Furnished Information (GFI) within software, hardware, and service components that monitor, identify and mitigate potential cyber security threats. The service monitors Internet traffic bound for or originating from the federal government, detects signs of malicious cyber activity, and prevents that traffic from jeopardizing the confidentiality, integrity, availability, and control of Participating Agency networks (i.e., agencies who enter into a Memorandum of Agreement with the Department of Homeland Security (DHS) to authorize the application of intrusion prevention capabilities by DHS and DHS contractors to approved agency traffic).

C.2.8.9.1 Service Description

C.2.8.9.1.1 Functional Definition

This service includes the following set of functions:

1. Indicator management
2. Detection
3. Response and Protection
4. Alerting and Reporting

Indicator management covers work necessary to manage and share cyber threat indicators and countermeasures. Detection covers access to network traffic and the application of a wide range of capabilities to inspect that traffic and identify malicious activity. Response and Protection functions cover capabilities that apply countermeasures to prevent and manage malicious activities. Alerting and reporting covers event notification and forensic artifact handling.

C.2.8.9.1.2 Standards

This service shall comply with the following standards and guidance:

- ICD 703 – Protection of Classified National Intelligence, Including Sensitive Compartmented Information
- NSA Security Guidelines for IPSS/ECS
- CNSSI 1253 – Security Categorization and Control Selection for National Security Systems, 27 March 2014
- NIST SP800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations
- CISA Incident Reporting System Standard Operating Procedures (SOPs) SOP 108 – Identifying Sensitive Information: PII Handling and Minimization, and SOP 110 - PII Handling & Minimization

The contractor may propose alternatives at no additional cost to the government that meet or exceed required technical capabilities; DHS Network Security Deployment security representatives should be consulted.

C.2.8.9.1.3 Connectivity

DHS IPSS shall connect with EINSTEIN Enclaves, examine Participating Agency traffic meeting the definition of “External Traffic” in TIC v2.0 and as described in Section C.1.8.8 paragraph 3, and connect to the CISA Incident Reporting System data centers.

C.2.8.9.1.4 Technical Capabilities

The DHS IPSS requires the following minimum, mandatory capabilities.

1. Establish and support a process that allows DHS to provide cyber threat indicators and define desired effects in the protection of covered network traffic.

2. Demonstrate to DHS that IPSS operates as intended when traffic is present that matches malicious indicators prior to the activation of new or modified indicators and their associated actions.

3. Support a process that allows DHS to direct actions on network traffic to gather additional information on cyber threats, stop cyber attacks, and/or respond to cyber incidents.

4. Provide for the ability to receive, accept, utilize, and secure GFI up to the Top Secret/Sensitive Compartmented Information (TS/SCI) level, including PII, such

as cyber threat indicators signatures, and associated actions in accordance with DHS-approved security guidelines.

5. Provide an automated means for DHS to share GFI and utilize the GFI provided within the DHS IPSS in as near real-time as possible.
6. Establish or leverage additional commercially available cyber threat information and/or DHS IPSS functional capabilities to provide additional protections for Federal Systems.
7. Ensure only those indicators and associated actions that are approved and further specified by DHS are applied to Participating Agencies.
8. Provide the ability to apply different sets of mitigation capabilities to a Participating Agency's traffic that does not affect which mitigations are applied to a separate Participating Agency's traffic.
9. Ensure that GFI is not disclosed or shared with any third party or used for any purpose that DHS has not specifically authorized.
10. Gain access to approved Participating Agency Federal System network traffic that uses the contractor as its Internet service provider.
11. Establish the ability to detect malicious network traffic to support the DHS IPSS and to provide additional contextual information associated with alerts to support post-incident analysis
12. Support signature-based, heuristic-based and/or other emerging detection methods.
13. Provide solutions that allow for the detection of malicious activity within encrypted traffic.
14. Support a wide-range of unclassified and/or classified protection measures. The kinds of protection measures the government expects to be available via a DHS IPSS can best be described by referencing the NIST Guide to Intrusion Detection and Prevention Systems. The guide defines typical IPSS capabilities as providing the capability to:
    - collect more detailed information for a specific session after malicious activity has been detected
    - prevent or block a detected threat by terminating the network connection or blocking access to the target
    - change the attack's content by removing or replacing malicious portions of an attack to make it inoperable
    - see evasion techniques and duplicate processing performed by a target

- tune detection accuracy so that an organization can achieve an optimum mix of false positives to false negatives in line with that organization’s risk tolerance

15. Include the ability to redirect to a safe server.

16. Allow for the capturing and storing of analytically relevant data associated with potential harmful network traffic specific to some indicators but and not necessarily applied to all indicators.

17. Ensure that the DHS IPSS technology does not retain traffic other than traffic associated with suspected malicious activity or as otherwise required by DHS.

18. Apply DHS-directed prevention services, as defined and approved by the Cybersecurity and Infrastructure Security Agency’s Cybersecurity Division.

19. Apply DHS-directed prevention services through an approved traffic segregation solution to only designated, Federal System network traffic.

20. Operate as an in-line service (i.e., a service within the ISP network boundary that is capable of performing mitigation actions as traffic traverses the ISP network in the normal flow of traffic) that detects and mitigates malicious IP-based traffic. For the purposes of this contract and to maximize contractor flexibility, the term “in line” should not be construed as mandating a specific network architecture, rather, the service should ensure that the following two conditions are met:

    a) All Internet traffic delivered to the Participating Agency’s SDP shall be monitored and subject to mitigation by the Prevention Service prior to said delivery.
    b) All Participating Agency traffic delivered to the Internet via the Participating Agency’s SDP shall be monitored and subject to mitigation by the Prevention Service prior to said delivery.

21. Define and apply the full range of existing and future DHS IPSS functional capabilities (typically defined in a technology roadmap) at cyber-relevant speed to counter cyber threats and attacks.

22. Provide quarantined malware to Participating Agency and to DHS via the CISA Threat Hunting malware lab or other specified DHS entity.

23. Prior to utilization of cyber threat indicators, signatures, and/or countermeasures, demonstrate to the government that cyber threat indicators, signatures, and/or countermeasures provided operate as intended.

24. Provide DHS and Participating Agencies with detection alerts and associated contextual information around suspicious traffic sufficient to identify the facts of a

particular incident or attempted incident for protected traffic in accordance with DHS specifications or guidance.

25. Provide DHS and Participating Agencies with data to support network traffic pattern assessments to detect and address anomalous patterns that may be indicators of malicious activity in accordance with DHS specifications or guidance.
26. Provide DHS and Participating Agencies with information related to indicators, signatures, associated actions, and/or alerts over a given time period.
27. Ensure that agency network traffic and other information are not disclosed to any party other than DHS and the agency and then only as specifically identified under this contract and task orders thereto, and take necessary steps to ensure Participating Agency data is secure from unauthorized access, use, disclosure, or retention.
28. Provide test results and support a process that allows for government participation and observation in tests.
29. Within 15 minutes of discovery, notify DHS of any unauthorized access, use, disclosure, or retention of Participating Agency data, and of any breach of any security or information handling requirements or additional instructions provided by DHS regarding the handling of Participating Agency network traffic, and provide relevant information to allow DHS to assess the scope of any such breach.
30. Provide an ICD 705 Sensitive Compartmented Information Facility (SCIF) and personnel with TOP SECRET/SCI clearances. Facility size, number of personnel and other details to be provided with DHS Task Orders.

C.2.8.9.2 Features

The following features are mandatory:

1. Classified Email Threat Detection and Countermeasures. The contractor shall provide capabilities that apply sensitive and classified (up to TS/SCI) indicators and countermeasures offered by DOD/DHS to email messages and with real-time secure exchange with DHS for global awareness.
2. Classified DNS Threat Detection and Countermeasures. The contractor shall provide capabilities that apply sensitive and classified (up to TS/SCI) indicators and countermeasures offered by DOD/DHS to DNS queries and responses and with real-time secure exchange with DHS for global awareness.

3. Additional countermeasures as specified by DHS.

C.2.8.9.3 Interfaces

The contractor shall support the UNI at the SDP to connect to the DHS IPSS as Ethernet Access defined in Section C.2.1.2.

C.2.8.9.4 Performance Metrics

Performance metrics for this service shall be defined in the TO.

C.2.8.10 Software Defined Wide Area Network Service (SDWANS) [Optional]

As agencies modernize and optimize their network infrastructure, many are considering a Software Defined WAN (SD-WAN) service. The benefits include cost-effectiveness, improved network management, increased routing flexibility, security, and network redundancy/availability/resiliency.

The Software Defined Wide Area Network Service (SDWANS) will support a wide range of connectivity requirements that enable government users to access cloud services, the Internet, government-wide intranets, and extranets, via EIS transport services. SDWANS will use the TCP/IP protocol suite to interconnect GFP/SRE with other government networks and the public Internet Service Provider (ISP) networks.

C.2.8.10.1 Service Description

The SD-WAN Service will create a transport agnostic overlay network to monitor, manage, and optimize the use of the underlying physical transport networks (underlays) for routing of session-based IP-packets by de-coupling the transport service from its applications and software control function in a separate control plane. The underlying transport can be any IP based service, including IPS, VPNS, ETS and BIS.

C.2.8.10.1.1 Functional Description

SDWANS shall support the following functions:

1. A secure IP-based virtual overlay network over physical IP networks (underlays) using an encrypted connection, compliant with the FIPS 140-2/3 standard for approved cryptographic modules.
2. Transport-independence of underlay network types, including IPS, VPNS, ETS and BIS.

3. Quality-of-Service (QoS) assurance of each FIPS 140-2/3 compliant encrypted connection is to be measured in real-time on key parameters (latency, packet loss, and jitter) to ensure that the performance level specified is being achieved.
4. Policy-based packet forwarding of different types of packet flows for QoS, security, and/or business policy for the best-matching transport underlay (physical network).
5. High availability through multiple underlays for transport diversity for increased overall availability and resiliency, including dynamic traffic routing to avoid network congestion and outage.
6. Zero touch provisioning of CPE (e.g. customer edge router) when powered up and connected by automatically retrieving its configuration and security policies without manual intervention.
7. Centralized management, including the ability to establish policies and monitor performance.

C.2.8.10.1.2 Standards

SDWANS shall comply with the following standards as solutions become commercially available:

1. Metro Ethernet Forum (MEF) on SD-WAN
    a. Standard
        i. MEF 70: SD-WAN Service Attributes and Services
    b. Supporting documents
        i. Presentation: MEF SD-WAN Services (MEF 70)
        ii. White Paper: Understanding SD-WAN Managed Services: Service Components, MEF LSO Reference Architecture and Use Cases
2. MEF CE3.0 for Carrier Ethernet
3. MEF 3.0 – Framework for dynamic Carrier Ethernet, SD-WAN, Optical Transport, IP, Security-as-a-Service, and other virtualized services
4. IETF RFCs for IPv6
5. IEEE:
    a. 802.1Q
    b. 802.1P
    c. (Optional) 802.3AD

6. Network Function Virtualization (NFV): ETSI ISG NFV Releases
7. All new versions, amendments, and modifications to the above documents and standards

C.2.8.10.1.3 Connectivity

SDWANS shall connect via underlays to:

1. Government locations, including mobile and remote users.
2. Physical IP-networks (underlays), such as IPS, VPNS, ETS, and BIS.
3. Connectivity to Government's Cloud Service Provider's SDP (see EIS Section C.2.5 Cloud Services)

C.2.8.10.1.4 Technical Capabilities

The following SDWANS capabilities are mandatory unless marked optional:

1. The contractor shall provide optional BIS required for the SDWANS at Agency sites, when specified in the Agency TO, at available data rates.
2. Tunnel virtual connection over the underlay networks
    a. SD-WAN shall provide a secure IP-based virtual overlay network that uses FIPS 140-2/3 compliant encrypted connection through one or more underlay networks. For additional security, the FIPS 140-2/3 compliant encrypted connection shall support Agency-provided end-to-end encrypted traffic.
    b. Underlay physical networks could be any IP networks, such as contractor-provided BIS, IPS, ETS, VPNS; including layer-1 transport, such as PLS.
    c. End-to-end secure FIPS 140-2/3 compliant encrypted connection shall also include Access Arrangements that connect Agency sites (SDPs) to their respective underlay physical network POPs.
3. Policy-Based Packet Forwarding
    a. Agencies shall be able to define policies to make application forwarding (or application-aware routing) decisions for SD-WAN tunnels over each underlay. Policies can be based on each application or application grouping, such as real-time media or conferencing application or non-real-time application.
        i. Performance Based Routing for multi-homed nodes (the best route is chosen based on real-time performance characteristics of the

network, such as jitter, latency, packet loss, and available bandwidth, for example to support VoIP traffic)

ii. Based on an agency's security or business policy requirements, for example:

1. Email replication, file transfer, and other bandwidth-intensive, latency-tolerant applications may be sent across an Internet path, while VoIP sessions, which are sensitive to jitter and packet loss, should be sent across MPLS.
2. Applications more critical to business should take priority over those less critical; and, VoIP and real-time applications should take precedence over backup.
3. Network segmentation for: Guest, Component-specific Intranet, Network management, and Legacy Application zones.

iii. Committed bandwidth (data rate) or CIR can be defined for each application flow.

4. Zero-Touch Provisioning of Site Equipment.
    a. Universal CPE (uCPE) or virtualized edge router for SD-WAN connectivity, when powered up and connected, shall automatically retrieve and install its configuration and policies without manual intervention. The uCPE (SRE) shall support Network Function Virtualization (NFV) capabilities for network routing functions and network security functions or via specialized appliances (SRE) if not supported.
    b. Agency specified security functions (e.g., Firewall, IDS/IPS, SBC) required by the edge router (uCPE) shall be provided via service-chaining of the EIS Managed Security Services (MSS) functions or catalog-based CLINs (e.g., Firewall, IDS/IPS, SBC).
5. Management and Control
    a. Ability to centrally define and update network monitoring, policy-setting, network segmentation, bandwidth allocation or CIR for each application flow, and other SD-WAN service profiles.

C.2.8.10.2 Features

The SDWANS features are mandatory unless marked optional.

ID Number	Name of Feature	Description
1 (Optional)	Online Management and Control (Partial)	In a co-managed environment, the Agency shall be able to control (define and update) aspects of the SD-WAN such as defining application flows and creating/modifying application flow policies via a service-specific web portal or application programming interface (API)
2 (Optional)	Online Management and Control (Full)	The Agency shall be able to define and update network monitoring, policy-setting, network segmentation, bandwidth allocation or committed information rate (CIR) for each application flow, and other SD-WAN service profiles via a service-specific web portal or application programming interface (API)
3 (Optional)	Advanced Analytics and Reporting	Advanced analytics to define and configure SD-WAN network architecture for increased reliability and security for a large Agency network, for example, 'big data' analytics of real-time performance metrics of all SD-WAN connections.

ID Number	Name of Feature	Description
4 (Optional)	Zero Trust Architecture (ZTA)	In the zero trust models, the notion of "trust anything" is abolished. This means no user, traffic source, or connected network are considered above suspicion, regardless of its location on or relative to the Agency network. All session-based network flows shall be authenticated and authorized. With session directionality built in, each route shall become a secure vector that tightly controls access to the destination or service; and, as specified in the Agency TO - for example, micro segmentations for and policy enforcement points (PEPs) at security boundaries, including defining security parameters, such as ACL, IDS/IPS, deep packet inspection, and flow control based on source, destination, application, and time-of-day. [Refer to "NIST SP 800-207 (Draft): Zero Trust Architecture" for deployment models and use cases.]

ID Number	Name of Feature	Description
5 (Optional)	Virtual Trusted Internet Connection (vTIC)	Virtual Trusted Internet Connection (vTIC) shall comply with current OMB TIC policy and shall support Traditional (conventional) TIC, Branch office, Cloud Service Provider, and Remote Access use cases (at a minimum) for high, medium, and low trust zones, as defined in the DHS CISA TIC 3.0 Reference Architecture Guidance and Security Capabilities Handbook. The security capabilities required for various TIC use cases may be based on EIS MSS catalog-based CLINs. The EIS MTIPS service may be leveraged to support TIC use cases where feasible, primarily when considering the Traditional TIC use case. Services shall be delivered as specified in the Agency TO.

ID Number	Name of Feature	Description
6 (Optional)	Network-as-a-Service (NaaS)	As virtualization continues to optimize the delivery of network functions, for example, as operational demands increase, functions can be scaled (e.g., bandwidth, capacity) and replicated across the environment. This will allow services to be optimally placed to meet demands or re-positioned to accommodate bottlenecks or outages in the underlying network fabric. The goal is to operate Agency networks as a next-generation, professionally managed and integrated infrastructure, and enterprise service as a NaaS with central control and management, by utilizing the evolving functionalities of SD-WAN, ZTA, SDN/NFV, PKI/CA as a service, and distributed-PEP at LAN, WAN, and Cloud edges/boundaries, instead of a choke point of single PEP at the Agency data center - as these capabilities mature and are available commercially.

C.2.8.10.3 Interfaces

The following UNIs at the SDP may be leveraged to connect the uCPE (e.g. virtualized edge router) to multiple underlays (e.g. BIS, IPS, VPNS and ETS services) with access arrangements to their respective POPs for the provisioning of SDWANS.

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type
1	Cable High Speed Access	25 Mbps download, 5 Mbps upload and above (DOCSIS 3.x or latest standard)	Point-to-Point Protocol, IPv4/v6

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type
2	Ethernet Interface	1. 1 Mbps up to 1 GbE (Gigabit Ethernet) 2. 10 GbE and above 3. Burstable	IPv4/v6 over Ethernet
3	IP over SONET Service	1. OC-3c 2. OC-12c 3. OC-48c 4. OC-192c	IP/PPP over SONET
4	Private Line Service	1. DS0 2. T1 3. T3 4. OC-3c 5. OC-12c 6. OC-48c 7. OC-192c	IPv4/v6 over PLS
5	DSL Service	xDSL access at 1.5 Mbps download and above, and 384 Kbps and above upload	Point-to-Point Protocol, IPv4/v6
6	FTTP	10 Mbps and above	Point-to-Point Protocol, IPv4/v6

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type
7	Wireless Access	1. 4G LTE 2. 5G and future evolutions 3. Wi-Fi 6 (IEEE 802.11ax) 4. Satellite	Point-to-Point Protocol, IPv4/v6

C.2.8.10.4 Performance Metrics

The performance levels (AQL and KPIs) for SDWANS are mandatory unless marked optional and are as follows:

1. For SDWANS overlay: As specified in the Agency TO:
2. For SDWANS underlays: Same as IPS, VPNS, and ETS services as follows:
   a. For VPNS, see Section C.2.1.1.4 VPNS Performance Metrics
   b. For ETS, see Section C.2.1.2.4 ETS Performance Metrics
   c. For IPS, see Section C.2.1.7.4 IPS Performance Metrics
   d. For BIS, see Section C.2.1.8.4 BIS Performance Metrics

The Table below applies to all SDWANS underlays:

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 1
	With Dispatch	8 hours	≤ 8 hours	

Notes:

1. See Section G.8.2 for the definitions and measurement guidelines.

C.2.9 Access Arrangements

C.2.9.1 Access Arrangement Description

Access Arrangements (AAs) connect the SDP at the agency location to a POP on the contractor's network. The range of line speeds and reliability options allows agency users to satisfy their diverse needs to access contractor networks. AAs provide the convention to specify and price the originating and/or terminating access component required to deliver a service. AAs cannot be ordered as a standalone access service and no performance metrics are specified for them.

C.2.9.1.1 Functional Definition

AAs can be used for any application such as voice, data, video, and multimedia. AAs shall provide diversity options that include, but are not limited to:

1. Physically disparate, diverse paths from the SDP to the POPs of two diverse contractors.
2. Physically disparate, diverse paths from the SDP to the contractor's POP.
3. Redundant paths from an SDP to the contractor's POP.

Special construction may involve providing a special service or facility related to the delivery and/or performance of a service requirement. This shall include the following situations:

1. An access arrangement does not exist or does not have sufficient capacity, and the contractor has to provide special construction through the implementation, rearrangement or relocation of physical plant solely for the government-requested access arrangement.
2. The contractor uses special construction to implement a different route (government premises to a PCL, PCL to an alternate contractor's POP, or some other type of route) than that which the contractor would otherwise use to provide an access arrangement for the government.

When necessary to fulfill an order, the contractor shall perform site surveys of potential operational locations to collect and validate floor plans, physical measurements, building power capacity, and external ingress/egress factors. The contractor shall deliver site survey reports after the completion of the physical site visits. See Section J.10 for the special access construction template for the site survey report.

C.2.9.1.2 Standards

AAs shall comply with the following standards:

1. ANSI T1.102/107/403/503/510 for T1
2. ANSI T1.607/610 for ISDN PRI
3. Telcordia PUB GR-499-CORE for T3
4. ANSI T1.105 and 106 for SONET
5. Telcordia PUB GR-253-CORE for SONET
6. ITU-TSS G.702 and related recommendations for E1 and E3
7. Frequencies grid and physical layer parameters for Optical Wavelength:
    a) DWDM: ITU G.692 and G.694 as mandatory and G.709 and G.872 as optional
    b) WDM: ITUG.694.2 and Telcordia GR 253
8. Applicable Telcordia for DWDM systems are GR-1073, GR-1312, GR-2918, GR-2979 and GR-3009
9. EIA/TIA-559, Single Mode Fiber Optic System Transmission Design
10. Telcordia GR-20-CORE for Generic Requirements for Optical Fiber and Optical Fiber Cable GR-253 (SONET), and GR-326 (Connector)
11. Digital Subscriber Line (DSL) - ADSL and SDSL:
    a) ADSL and DSL Forums
    b) ITU-TSS Recommendation G.992 for ADSL (interoperable DSL modem and DSLAM line card)
    c) ANSI T1.413 (compatible DSL modem and DSLAM line card from the same manufacturer)
12. ISDN based DSL (IDSL): ISDN Forums
13. Ethernet Access: IEEE 802.3, including 10 Base-T/TX/FX, 100 Base-TX/FX, 1000 Base-T/FX/L/LX/B/BX/PX, and 10/40/100 Gigabit Ethernet (IEEE 802.3ae and 802.3ba)
14. Cable High-Speed Service: DOCSIS (Cable Labs) standards
15. The contractor shall comply with all new versions, amendments, and modifications to the above documents and standards

C.2.9.1.3 Connectivity

AAs shall connect to and interoperate with:

1. Agency-specified locations and equipment
2. Contractor's network POPs

C.2.9.1.4 Technical Capabilities

The following AA capabilities are mandatory unless marked optional:

1. Integrated access of different services
2. Transparent to any protocol

The following AAs are mandatory unless marked optional:

1. **T1**. A line rate of 1.544 Mbps, which may be used to provide channelized or unchannelized T1 access arrangement as follows:
   a) Channelized T1. In this mode, 24 separate DS0s clear channels of 56/64 kb/s shall be supported.
   b) Unchannelized T1. In this mode, a single 1.536 Mbps information payload shall be supported.
2. **ISDN PRI**. This category of AA shall support 23 separate DS0 clear channels of 56/64 kbps over an interface of ISDN PRI (23B+D) with a line rate of 1.544 Mbps.
3. **ISDN BRI**. This category of AA shall support 2 separate DS0 clear channels of 56/64 kbps over an interface of ISDN BRI (2B+D) with a line rate of 144 Kbps.
4. **T3**. This category of AA shall support a line rate of 44.736 Mbps, which may be used to provide channelized or unchannelized T3 access arrangement as follows:
   a) Channelized T3. In this mode, 28 separate DS1 channels of 1.536 Mbps information payload rate shall be supported.
   b) Unchannelized T3. In this mode, a single 43.008 Mbps payload shall be supported.
5. **E1** This category of AA shall support a line rate of 2.048 Mbps, which may be used to provide channelized or unchannelized E1 service as follows:
   a) Channelized E1. In this mode, 30 separate DS0 clear channels shall be supported.
   b) Unchannelized E1. In this mode, a single 1.92 Mbps information payload shall be supported.

6. **E3** This category of AA shall support a line rate of 34.368 Mbps, which may be used to provide channelized or unchannelized E3 service as follows:

    a) Channelized E3. In this mode, 16 separate E1 channels shall be supported.

    b) Unchannelized E3. In this mode, a single 30.72 Mbps information payload shall be supported.

7. **SONET OC-3. T**his category of AA shall support a line rate of 155.520 Mbps, which may be used to provide channelized OC-3 or concatenated OC-3c access arrangement as follows:

    a) Channelized OC-3. In this mode, three separate OC-1 channels, each with an information payload data rate of 49.536 Mbps, shall be supported.

    b) Concatenated OC-3c. In this mode, a single channel equivalent to information payload data rate of 148.608 Mbps shall be supported.

8. **SONET OC-12**. This category of AA shall support a line rate of 622.080 Mbps, which may be used to provide channelized OC-12 or concatenated OC-12c access arrangement as follows.

    a) Channelized OC-12. In this mode, 4 separate OC-3 channels, each with an information payload data rate of 148.608 Mbps, shall be supported.

    b) Concatenated OC-12c. In this mode, a single channel equivalent to an information payload data rate of 594.432 Mbps shall be supported.

9. **SONET OC-48**. This category of AA shall support a line rate of 2.488 Gbps, which may be used to provide channelized OC-48 or concatenated OC-48c service as follows:

    a) Channelized OC-48. In this mode, 4 separate OC-12 channels, each with an information payload data rate of 594.432 Mbps, shall be supported.

    b) Concatenated OC-48c. In this mode, a single channel equivalent to an information payload data rate of 2.377728 Gbps shall be supported.

10. **SONET OC-192**. This category of AA shall support a line rate of 10 Gbps, which may be used to provide channelized OC-192 or concatenated OC-192c service as follows:

    a) Channelized OC-192. In this mode, 4 separate OC-48 channels, each with an information payload data rate of 2.488 Gbps, shall be supported.

    b) Concatenated OC-192c. In this mode, a single channel equivalent to an information payload data rate of 9.510912 Gbps shall be supported.

11. **(Optional) SONET 768**. This category of AA shall support a line rate of 40 Gbps, which may be used to provide channelized OC-768 or concatenated OC-768c service as follows:

a) Channelized OC-768. In this mode, 4 separate OC-192 channels, each with an information payload data rate of 9.510912 Gbps, shall be supported.

b) Concatenated OC-768c. In this mode, a single channel equivalent to an information payload data rate of 38.486016 Gbps shall be supported.

12. (Mandatory if CSVS or PLS analog transport is offered, optional otherwise) **Analog Line (4 KHz)**. This category of AA shall support 2 wire analog lines and trunks without access integration for voice service.

13. **DS0**. This category of AA shall support information payload data rates of 56 kbps and 64 kbps.

14. **(Optional) Subrate DS0**. This category of AA shall support Subrate DS0 at information payload data rates of 4.8, 9.6, and 19.2 kbps.

15. **Optical Wavelength**. Bi-directional wavelengths (WDM) connections to an optical network for the following speeds:

    a) 1 Gbps.

    b) 2.5 Gbps.

    c) 10 Gbps.

    d) 40 Gbps and above (Optional).

16. **(Optional) Dark Fiber**. Dark Fiber shall support the following capabilities:

    a) Deployed fiber shall support both single-mode and multimode fibers.

    b) Deployed fibers shall be capable of supporting a minimum of 80 DWDM wavelengths or user data with spacing as specified in ITU-T G.694.1.

    c) Deployed fibers shall be capable of operating in the "C", ”D”, “L” and ”S” bands.

17. **Digital Subscriber Line** (DSL) Access Arrangements:

    a) Provide the following types of DSL services, at a minimum:

        1. Asymmetric DSL (ADSL). Support ADSL asymmetric data rates for upload and download traffic as follows:
            - Upload: Data rates shall range from 16 to 768 kbps (e.g., 256 kbps).
            - Download: Data rates shall range from 1.5 Mbps to 8 Mbps (e.g., at 1.5, 2, 3, 4, 5, 6, 7, and 8 Mbps). Speeds up to 50 Mbps are optional.
        2. Symmetric DSL (SDSL). Support SDSL symmetric (i.e., same) data rates for both upload and download traffic at data rates up to and including 1.5 Mbps. 2.3 Mbps is optional
        3. (optional) ISDN DSL (IDSL). Support ISDN symmetric (i.e., same) data rates for both upload and download traffic at data rates of 144 Kbps.

18. **Ethernet** Access Arrangements:

    a) Ethernet Access Arrangements shall support both dedicated access and/or shared access (multiplexed Ethernet connections) over a Metro Ethernet service from SDP to POP. The contractor shall support access speeds of:

    1. 1 Mbps to 10 Mbps at 1 Mbps increments
    2. 10 Mbps to 100 Mbps at 10 Mbps increments
    3. 100 Mbps to 1 Gbps at 100 Mbps increments
    4. (Optional) 2 Gbps to 10 Gbps at 1 Gbps increments
    5. (Optional) 10 Gbps to 100 Gbps at 10 Gbps increments and above

    For each of the access connections, the contractor shall maintain appropriate committed bandwidth or CIR (Committed Information Rate), as supported by the MEF 33 - Ethernet Access Services standard and the MEF Bandwidth Profiles for Ethernet Services and as specified in the TO.

19. **(Optional) Cable High-Speed** Service Access Arrangements:

    a) Provide data rates of 25 Mbps download, 5 Mbps upload and above (DOCSIS 3.x or latest standard)

20. (Optional) Fiber-To-The-Premises (FTTP):

    a) 25 Mbps (download) and 5 Mbps (upload) and above

21. **Wireless** Access Arrangements:

    a) Cellular Service - 4G Long Term Evolution (LTE), 5G, and future evolutions:

    1. 100 mbps (download), 50 mbps (upload) and above

    b) Line of sight connection, using licensed frequencies:

    1. DS1
    2. NxDS1 (where N=2 through 27)
    3. DS3
    4. E1 (Non-domestic)
    5. NxE1 (where N=2 through 15) (Non-domestic)
    6. E3 (Non-domestic)
    7. SONET OC-3
    8. 1 Gbps, 5 Gbps and 10 Gbps

C.2.9.2 Access Diversity and Avoidance

The following are mandatory unless marked optional.

ID Number	Name of Access Capability	Description
1	Access Route or Path Diversity	The contractor shall supply at least two physically-separated routes for access diversity with the following options: 1. Between an SDP and its associated connecting network's PCL or POP, or 2. Between an SDP and at least two connecting network PCL/POPs. 3. Access from the same or different access providers (e.g., ILEC and a CLEC) for two separate routes, using any mix of access arrangements. These diverse routes shall: 1. Not share any common telecommunications facilities or offices including a common building entrance. 2. Maintain a minimum separation of 30 feet throughout all diverse routes between premises/buildings where an SDP and its associated network connecting point are housed. 3. Maintain a minimum vertical separation of two feet, with cables encased (separately) in steel or concrete for cable crossovers. The contractor shall provide the capability for the automatic switching of transmission in real-time, negotiated on an individual case basis: 1. From the primary access route to the one or more diverse access routes, including satellite connection, and 2. From the diverse access route to the primary access route. The contractor shall exercise the following control measures on the configuration or the reconfiguration of the diverse access route: 1. The contractor shall provide a graphical representation (e.g., diagrams, maps) of access circuit routes to show where diversity has been implemented to the OCO within 30 calendar days of the implementation of access diversity and again thereafter when a change is made. 2. Prior to any proposed reconfiguration of routes previously configured for access diversity, the contractor shall provide to the agency written notification and revised PCLs for OCO approval in accordance with the requirements of the TO. 3. The contractor shall establish internal controls to prevent the dismantling of diversified routes.
2	Access Route or Path Avoidance	The contractor shall supply the capability for a customer to define a geographic location or route to avoid between an SDP and its associated connecting network point.

ID Number	Name of Access Capability	Description
		The contractor shall exercise the following control measures on the configuration or reconfiguration of the avoidance access route: 1. The contractor shall provide a graphical representation (e.g., diagrams, maps) of access circuit routes to show where avoidance has been implemented to the OCO within 30 calendar days of the implementation of avoidance and again thereafter when a change is made. 2. Prior to any proposed reconfiguration of routes previously configured for avoidance, the contractor shall provide to the agency written notification and revised PCLs for OCO approval in accordance with the requirements of the TO. 3. The contractor shall establish internal controls to prevent the dismantling of avoided routes.

C.2.9.3 Interfaces

The UNIs at the SDP for AA are mandatory unless marked optional:

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	ITU-TSS V.35	Up to 1.92 Mbps	Transparent
2	EIA RS-449	Up to 1.92 Mbps	Transparent
3	EIA RS-232	Up to 19.2 kbps	Transparent
4	EIA RS-530	Up to 1.92 Mbps	Transparent
5	T1 (with ESF) [Std: Telcordia SR-TSV-002275; ANSI T1.403)	Up to 1.536 Mbps	1. Transparent 2. IP (v4/v6)
6	ISDN PRI (23B+D and 24B+0D) [Std: ANSI T1.607/610]	Up to 1.472 Mbps	Transparent
7	T3 [Std: Telcordia GR-400-CORE]	Up to 43.008 Mbps	Transparent
8	E1 (Std: ITU-TSS	Up to 1.92 Mbps G.702) (Non-domestic)	Transparent

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
9	E3 (Std: ITU-TSS G.702) (Non-domestic)	Up to 30.72 Mbps	Transparent
10	SONET OC-3 (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
11	SONET OC-3c (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
12	SONET OC-12 (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
13	SONET OC-12c (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
14	SONET OC-48 (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent
15	SONET OC-48c (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent
16	SONET OC-192 (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent
17	SONET OC-192c (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent
18	SONET OC-768 (Std: ANSI T1.105 and 106)	38.486016 Gbps	Transparent
19	SONET OC-768c (Std: ANSI T1.105 and 106)	38.486016 Gbps	Transparent
20	10 Base-T/TX/FX (Std: IEEE 802.3)	Link bandwidth: Up to 10 Mbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
21	100 Base-TX/FX (Std: IEEE 802.3)	Link bandwidth: Up to 100 Mbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
22	1000 Base-T/L/LX/B/BX/PX (Std: IEEE 802.3)	Link bandwidth: Up to 1 Gbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
23	10 Gbps (Std: IEEE 802.3)	Link bandwidth: Up to 10 Gbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
24	Reserved		
25	ISDN BRI (2B+D) (Multirate) [Standard: ANSI T1.607 and 610]	144 kbps	1. ITU-TSS Q.931 2. IP (v4/v6)
26	3G / 4G LTE / 5G and future evolutions (Cellular Service)	Up to current standard	1. IP (v4/v6)

C.2.10 Service Related Equipment

When identified in a TO, the contractor shall provide networking and security service-related equipment such as Switches, Routers, PBXs, Telephones, Servers, Security Appliances, Firewalls, Conferencing-Related Equipment, Microwave Systems, Free-space Optics Systems, Surveillance Systems, Sensors, Radio-related Equipment, VSATs, and Wireless Devices.

The contractor shall provide hardware and materials that are incidental to the installation, operation and maintenance of EIS services.

All equipment provided to the government under this contract shall be new and not previously used or refurbished except when all of the following conditions are met:

- The incumbent under a legacy telecommunications contract/order is awarded a task order under EIS;
- The equipment was being paid for using an installment MRC under a legacy telecommunications contract/order;
- The agency awarding the task order requests that the contractor transfer the equipment from the legacy telecommunications contract/order to a task order placed against this contract.

C.2.10.1 Warranty Service

The contractor shall provide, at no additional cost to the government, a minimum one-year system warranty (or the warranty provided by the OEM, whichever is longer) for all hardware and software ordered under this contract, including all equipment supplied, installed, and integrated by the contractor. The equipment warranty shall provide for hardware repairs and the distribution of updated software to all users who ordered the hardware or software under this contract. The contractor shall provide warranty information associated with each product and service delivered to the GSA CO or OCO if requested.

The contractor shall repair or replace malfunctioning equipment covered by warranty within five (5) business days or as specified in the TO. The contractor shall provide to the government a point of contact for the warranty who is available from 7AM – 7PM local time, or for a longer period if specified in the TO. The warranty shall begin at the time the SRE is accepted.

C.2.11 Service Related Labor

The EIS services defined in Sections C.2.1 through C.2.10 and in Section C.2.12 include all service-related labor necessary to implement the services. Agencies may include labor on TOs to support services on this contract. Labor for construction, alteration, and repair is only in-scope as necessary to offer a complete solution, provided that such labor is integral to and necessary for the effort defined in the TO.

C.2.12 Cable and Wiring

The contractor shall provide installation services for equipment necessary to provide telecommunications services and related supporting IT services.

The contractor shall provide required connectivity using appropriate cabling and wiring, and related trenching, ducting, grounding, and lightning protection systems in accordance with the TO and appropriate standards.

Site preparation work done by the contractor under this contract shall conform to applicable federal, regional and local codes and shall conform to accepted industry installation and construction practices. All planned work and code compliance shall be subject to OCO review and approval prior to the start of work. The contractor shall provide the tools and test equipment to perform the site preparation as specified in the TO, and shall retain ownership of the tools and test equipment unless otherwise specified in the TO. The government will furnish facilities and utilities to the contractor that already are installed at the site, including light, heat, ventilation, and power. The contractor shall provide temporary utilities that are not available in the work area and coordinate any disconnection of utilities. The contractor shall provide building additions and/or changes as required to support the telecommunications and IT installation, provided they are integral to and necessary for the effort defined in the TO. HVAC and electrical construction shall be limited to new or upgraded installations necessary to support telecommunications and IT equipment. The contractor shall expand or modify power systems to provide appropriate environmental controls to support the installation.

The contractor shall provide a warranty period of at least one (1) year for the premises wiring/cabling after service acceptance.

C.3 Transition

In the general sense of the term “transition,” the government can move active services to EIS from any contract or agreement other than EIS, or from EIS to another contract or agreement. However, for the purposes of the EIS program, transition is more narrowly and specifically defined to allow clear and effective tracking of transition progress from certain expiring contracts. Therefore, EIS addresses two types of transition, “transition on” and “transition off,” which are defined as follows:

1. “Transition on” is the transfer of service from a Networx contract or a GSA Local Services Agreement (LSA) to the EIS contract.
2. “Transition off” is the transfer of service from the EIS contract to a follow-on contract or service arrangement, managed by GSA in a coordinated way to prepare for the expiration of the EIS contract, conducted as specified in FAR Clause 52.237-3.

C.3.1 Transition Roles and Responsibilities

C.3.1.1 Government’s Role in Transition

GSA will oversee transition activities to ensure they are progressing and issues are escalated as needed. The functions to be performed by GSA include the following:

1. Develop and publish a Transition Strategy and Management Plan (TSMP) for all stakeholders to have a common understanding of the goals of transition and GSA’s approach to managing transition across the government.
2. Monitor contractor’s performance according to the Transition Management Approach of the Program Management Plan (Section G.9.4) and initiate corrective action if required.
3. Support agencies as resources permit, according to an agreed-upon approach to transition assistance.
4. Coordinate with contractors and agencies to guide the sequence of transition orders to achieve early progress, level resource demands, and minimize backlogs.
5. Track and report on transition progress to all stakeholders and initiate corrective action as required.
6. Monitor and facilitate coordination and cooperation among the contractor, agencies, and other GSA contractors.

The agency will manage EIS transition activities to ensure that replacement services and disconnects are being implemented in a timely and effective manner, with minimal impact to the agency's operation. Many government organizations are decentralized; therefore, multiple entities within a department or an independent agency may perform the functions of an "agency." The agency's responsibilities and functions may be delegated to another agency, to a sub-agency or an agency component, or to a support contractor authorized to act on behalf of the agency. The functions to be performed by the agency for transition include the following:

1. Validate existing inventory to ensure it is accurate and current.
2. Evaluate current technical solutions and develop transition planning for target technical solutions, including upgrades, transformations, retirement, or other changes.
3. Develop an Agency Transition Plan and identify transition manager(s).
4. Communicate transition goals, telecommunications requirements, and existing inventory to the contractor throughout the ordering process, including within agency solicitations.
5. Monitor the contractor's transition performance, accept or reject services in accordance with Section E Inspection and Acceptance, and coordinate corrective actions with the contractor and GSA if required
6. Monitor and facilitate coordination between the contractor and Local Government Contacts (LGCs) and other agency vendors and service providers.

C.3.1.2 Contractor's Role in Transition

The contractor shall manage transition activities as described in its Program Management Plan. Except where specified further in this section, the contractor shall deliver all services transitioning onto EIS and disconnect services transitioning off EIS according to the same ordering and performance requirements the EIS contract specifies for those services.

C.3.2 Transition On

C.3.2.1 Objectives

GSA expects to define a phased approach for an orderly transition that completes within three (3) years of award of the contract. Furthermore, GSA intends to encourage agencies to enhance or transform services as well as to order new services in conjunction with transitioning services. Therefore, GSA will not require agencies or contractors to identify orders specifically as "transition." Rather, the contractor should ascertain through its order processing practices which services on an order are replacing active services on another contractual vehicle, and give those orders the appropriate attention to minimize impact on the ordering agency's operations when cutting over to the replacement service.

C.3.2.2 Contract-Wide Planning and Implementation

The contractor shall participate in planning with GSA and conduct transition planning and implementation that are consistent with GSA's TSMP to the extent possible. Certain phases may necessitate contractor personnel being dedicated to focus on those phases and interact with dedicated government personnel. As required by GSA for a phase, the contractor shall identify its personnel by name and contact information. The contractor shall train or orient GSA's transition personnel to use any self-help tools or systems the contractor makes available to agencies for transition and implementation.

C.3.2.3 Agency-Specific Planning and Implementation

The contractor shall respond to agency solicitations with solutions that best address the requirements of the agency to replace its existing services with solutions of equal or better levels of performance, ease of use, and cost effectiveness. The contractor should consult with the agency as appropriate throughout the acquisition process to determine the most effective method of transitioning from existing services to replacement services on EIS, while minimizing impact to the agency's operations. The contractor shall assist ordering agencies with placing TOs and service orders to ensure accuracy, completeness, and timeliness and to minimize delays in transitioning. The contractor shall coordinate with all incumbent contractors according to industry best practices.

C.3.2.4 Inventory

Each agency will compile its own transition inventory of existing services provided by the incumbent contractor. GSA will share with the agency any available information regarding those services and assist the agency in collecting and validating its inventory.

C.3.3 Transition Off

C.3.3.1 Objectives

This section describes the requirements for transitioning services from this contract to a follow-on vehicle.

C.3.3.2 Planning and Implementation

The contractor shall conduct transition planning with GSA and provide advice on strategies to minimize the transition time. The contractor shall perform PIC/LPIC changes in support of transition from EIS to a follow-on contract. The contractor shall accept a Letter of Authorization (LOA) from the agency to allow the follow-on contractor to order PIC/LPIC changes, including release of PIC freeze.

C.3.3.3 Inventory

In preparation for transition off this contract, the government must have a complete and accurate Transition Inventory. A Transition Inventory is a complete record of the services, features, equipment, location data, configuration information, and delivery description necessary to facilitate the transition of an agency's services. For solutions with delivery details that are more transparent to the user – such as TUCs, managed services, or cloud services – the delivery description shall include the functional solution and performance specification of the service rather than specific components.

If GSA exercises all the contract options, for the final five (5) years of the contract, the contractor shall conduct periodic validations (approximately once every 6 months) of its Transition Inventory with GSA and reconcile any discrepancies. If GSA exercises all the contract options, for the final three years of the contract the contractor shall conduct monthly validations with GSA. At the GSA CO's request, the contractor shall deliver an inventory summary of all services active – that is, in service, whether in use or not – at the time of the request, by AB code, service, quantity, and location. At the OCO's request, the contractor shall deliver an inventory summary of all the agency's services active at the time of the request.

C.3.3.4 Reporting

If GSA exercises all the contract options, for the final three (3) years of the contract, the contractor shall deliver weekly reports of services disconnected and active services based upon the transition inventory.

During that same three-year period the contractor shall deliver a monthly Transition Status Report that includes the following:

- Data file of invoiced amount by AB code for the most recently completed billing period
- Discussion of transition issues reported by agency customers or experienced by the contractor either during the reporting period or unresolved since the last report, corrective action, and status
- Risk analysis and response plan.

C.4 Section 508 Requirements

C.4.1 Background

Section 508 is the statutory section of the Rehabilitation Act of 1973 that requires federally procured Electronic Information Technology (EIT as defined in FAR 2.101) to provide disabled federal employees with access to and use of information that is comparable to information provided to nondisabled federal employees. Section 508 also requires federal agencies to provide disabled public citizens with access to and use of information that is comparable to information provided to nondisabled public citizens. For additional information see www.section508.gov.

The Access Board is an independent federal agency that established the standards for federally procured EIT products and services. The requirements that must be met consist of Technical Standards, Functional Performance Criteria, and Information, Documentation, and Support.

Agencies may accept EIT that uses designs and/or technologies that do not meet applicable Technical Standards but do provide disabled federal employees or citizens with equivalent or greater access to information. This is referred to as “equivalent facilitation” and vendors offering equivalent facilitation will be considered along with those that strictly meet the Technical Standards.

Revised Standards - As of January 18, 2018, Federal agencies must comply with the revised 508 Standards, which were issued by the U.S. Access Board in January 2017. These revised standards are set forth in 36 C.F.R. § 1194.1 and Appendices A, C and D to Part 1194. Information and communication technology (ICT) developed, maintained, or used by Federal agencies on or after this date must satisfy the updated scoping and technical requirements in the Revised 508 Standards. These Standards may be found at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines

Safe Harbor - The Revised 508 Standards also include a “safe harbor” provision for existing (i.e., legacy) ICT. Under this safe harbor, unaltered, existing ICT (including electronic content) that complies with the Original 508 Standards need not be modified or upgraded to conform to the Revised 508 Standards. This safe harbor applies on an element-by-element basis to each component or portion of the existing ICT, with each component or portion assessed separately. Existing, unaltered ICT that did not comply with the Original 508 Standards as of January 18, 2018 must now be brought into compliance with the Revised 508 Standards.

C.4.2 Voluntary Product Accessibility Template

The contractor shall post the Voluntary Product Accessibility Template (VPAT) for each service identified in paragraphs C.4.4 below to its web site, in order to demonstrate that offerings comply with Section 508 standards. The VPAT is required 30 days after NTP and is updated as needed. This will assist the customer agency in evaluating services for Section 508 standard compliance.

C.4.3 Section 508 Applicability to Technical Requirements

The Technical Requirements section (Section C.2) of the contract identifies the technical provisions for services used by an agency to execute mission operations. Services that execute mission operations shall meet the relevant provisions as identified in Section C.4.4 or shall provide equivalent facilitation. For less than fully compliant products see Section G.5.3.1.3.

C.4.4 Section 508 Provisions Applicable to Technical Requirements

The relevant provisions of Part 1194 Appendix A Chapter 1 Application and Administration and Chapter 2 Scoping Requirements along with Part 1194 Appendix C Chapter 3 Functional Performance Criteria, Chapter 4 Hardware, Chapter 5 Software, Chapter 6 Support Documentation and Services, and Chapter 7 Referenced Standards, shall apply to the appropriate EIS software, hardware, and web-based services, to include but not be limited to the following:

- Data Service.
- Voice Service.
- Managed Service.
- Contact Center Service.
- Data Center Service.
- Cloud Service.

The relevant provisions of Part 1194 Appendix C Chapter 3, Functional Performance Criteria, shall apply to appropriate services provided under the EIS contract. For the relevant services, the contractor shall provide one of the following two capabilities:

1. Support for assistive technologies used by disabled individuals.
2. At least one mode of operation and information retrieval that:
    a) For blind users, does not require vision.
    b) For vision impaired users, does not require visual acuity greater than 20/70.
    c) For deaf users, does not require hearing.

d) For hearing impaired users, does not require enhanced auditory capability.

e) For users with no speech capability or with impaired speech, does not require user speech.

f) For users without fine motor control or simultaneous action capability, does not require fine motor control or simultaneous action and is operable without limited reach and strength.

The relevant provisions of Part 1194 Appendix C Chapter 6 Support Documentation and Services, shall apply to the appropriate services provided under the EIS contract.

C.4.5 Section 508 Provisions Applicable to Reporting and Training

The government's information reporting requirements are addressed in Section G.9 Program Management. Required information shall be reported via the Internet, email, or telephone. Services providing the required information shall meet the relevant provisions of Part 1194 Appendices A and C or shall provide equivalent facilitation.

Training requirements are outlined in Section G.10 Training shall be delivered via meeting and briefings, classroom, seminars, instructor-led and non-instructor on-line web based self-study, and manuals or desk top guides. For training delivered via meeting and briefings, classroom, and seminars, assistance such as signers and Braille products shall be provided to disabled trainees when requested in advance by the government. For training delivered via instructor-led and non-instructor on-line web based, the same capabilities provided for Internet reporting shall be provided to disabled trainees.