Attachment B
SCOPE OF WORK

This Scope of Work (SOW) describes the Deliverables being sought through this RFP and the scope of what Contractors will be expected to offer through a Master Agreement (MA) resulting from this RFP. The Scope of Work is intended to provide potential Offerors with sufficient basic information to submit a proposal. It is not intended to limit a proposal's content or exclude any relevant or essential data.

I. BACKGROUND AND SOW OBJECTIVES

A. Background: The Data Communications portfolio has been solicited and awarded by the Lead State of Utah for the previous iteration which will be expiring on September 30, 2026. RFxPremier is a new cooperative that will be managing this portfolio in conjunction with the Lead Entity of Montana. This portfolio has a proven track record of providing data communications hardware, software, services, peripherals, etc. with a goal of offering total solutions to all interested purchasing entities who depend on data communications capabilities. There is a very strong user base and the need for secure information connected solutions under this portfolio. The new iteration under RFxPremier has a goal to ensure quality of offerings that are included in this scope of work.

Recognizing the landscape of the advancements in the industry, this solicitation and resulting MAs strongly encourage the Contractor to provide the most cutting edge and emerging technology that falls underneath the definition of Data Communications to provide advanced networks and systems from a holistic full solution approach.

B. Scope of Work Objectives:

1. Data Communications: For the purposes of this Scope of Work and the resulting Master Agreements, **Data Communications is defined as the products and services that provide the technological capabilities to transmit, receive, and manage digital information through information technology networks.** This SOW seeks the Contractor to provide all aspects of data communications capabilities in a holistic solution, that includes hardware, software, and services, to develop, establish, maintain, secure, and expand data communications networks.

2. Original Equipment Manufacturer (OEM): For the purposes of this Scope of Work and the resulting Master Agreements, **OEM is defined as a Contractor that designs and manufactures data communications hardware.** The OEM (Awarded Contractor) shall provide data communications solutions consisting of the hardware as well as software solutions and services to support the hardware. Offerors are strongly encouraged to review this definition as it pertains to this SOW, to determine its eligibility to submit a proposal. All Offerors must affirm their OEM status (as defined in this section) in Attachment G, Offeror Response Worksheet.

C. Approach and Considerations: The scope of work approach will not establish individual product award categories but will seek to award to OEMs that manufacture data communications

hardware and be capable of supporting that hardware through a holistic approach of software, cloud networking, services, etc. to provide the interested Participating Entities secure data communications capabilities in various protocols (data formatting, transmission, and error handling such as TCP/IP, HTTP, FTP, etc.). As stated, there will not be individual award categories, however, this SOW seeks solutions to be provided consisting of, but not limited to, the following common Data Communication fields:

- **Networking:** The infrastructure and systems that enable connectivity and data transfer, including routers, switches, network management and network optimization tools.
- **Unified Communications:** Data Communications products and technologies that integrate various communications to provide the capability of exchanging digital information seamlessly including, but not limited to, voice, video, and text and other forms of media.
- **Wireless Networking:** Technologies that enable data communication over wireless mediums, including Wi-Fi access points, wireless controllers, and related management tools.
- **Security:** Solutions that ensure confidentiality, integrity, and availability of data and network resources, including firewalls, intrusion detection/prevention systems, encryption technologies, and secure access controls.
- **Facilities Management:** Products and technologies that provide digital capabilities to manage, monitor, and control various facilities functions utilizing access control systems, security and surveillance, energy and climate control, alert and emergency response systems, etc.

The definition of Data Communications above will consist of the following and defined in the below sections of this SOW. Some content and scope in the sections may cross between hardware and software.

- Hardware
- Software
- Services

This Scope of Work is meant to be solution-based, the following content in this SOW is meant to provide guidelines and framework for Data Communications solutions, it is not meant to limit the scope or restrict the solutions or systems. It is strongly encouraged to propose emerging technologies (such as Artificial Intelligence, Internet of Things) under the multiple categories so long as it is considered within the scope of Data Communications, by the definition encompassing this SOW, and adds or enhances the overall solution for the customer. The products must be able to address customers' business needs and integrate into the overall solution.

II. DATA COMMUNICATIONS: HARDWARE

A. Networking: Routers – A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's

network. Routers are located at gateways, the places where two or more networks connect, and are the critical device that keeps data flowing between networks and keeps the networks connected to the Internet. Below is a list of routers, this list is not limited to the routers that can be provided under this scope:

1. **Branch Routers** — A multiservice router typically used in branch offices or locations with limited numbers of users and supports flexible configurations/feature. For example: security, VoIP, wan acceleration, etc.
2. **Network Edge Routers** — A specialized router residing at the edge or boundary of a network. This router ensures the connectivity of its network with external networks, a wide area network or the Internet. An edge router uses an External Border Gateway Protocol, which is used extensively over the Internet to provide connectivity with remote networks.
3. **Core Routers** – High performance, high speed, low latency routers that enable Enterprises to deliver a suite of data, voice, and video services to enable applications such as Internet Protocol Television (IPTV) and Video on Demand (VoD), and Software as a Service (SaaS).
4. **Service Aggregation Routers** — Provides multiservice adaptation, aggregation and routing for Ethernet and IP/MPLS networks to enable service providers and enterprise edge networks simultaneously host resource-intensive integrated data, voice and video business and consumer services.
5. **Carrier Ethernet Routers** — High performance routers that enable service providers to deliver a suite of data, voice, and video services to enable next-generation applications such as IPTV, Video on Demand (VoD), and Software as a Service (SaaS)

B. **Networking: Switches –** A networking hardware device that connects multiple technology devices within a local area network (LAN). It forwards data packets to the correct destination device, ensuring efficient communication. These can be managed, unmanaged, layer 2/3 devices that are used to connect segments of a LAN (local area network) or multiple LANs and to filter and forward packets among them. Below is a list of switches, this list is not limited to the switches that can be provided under this scope:

1. Campus LAN – Access Switches — Provides initial connectivity for devices to the network and controls user and workgroup access to internetwork resources.
2. Campus LAN – Core Switches — Campus core switches are generally used for the campus backbone and are responsible for transporting large amounts of traffic both reliably and quickly.
3. Campus Distribution Switches — Collect the data from all the access layer switches and forward it to the core layer switches. Traffic that is generated at Layer 2 on a switched network needs to be managed or segmented into Virtual Local Area Networks (VLANs), Distribution layer switches provides the inter-VLAN routing functions so that one VLAN can communicate with another on the network. Distribution layer switches provide advanced security policies that can be applied to network traffic using Access Control Lists (ACLs).

4. Data Center Switches — Data center switches, or Layer 2/3 switches, switch all packets in the data center by switching or routing good ones to their final destinations, and discard unwanted traffic using Access Control Lists (ACLs) a minimum of 10 Gigabit speeds. High availability and modularity differentiate a typical Layer 2/3 switch from a data center switch. Ability to remotely disable and enable individual ports. Support "NetFlow" or equivalent. Jumbo frame supports EVPN over MPLS or BGP (9k bytes), plug and play fabric formation. Ultra-low latency through wire-speed ports with nanosecond port-to-port latency and hardware- based Inter-Switch Link (ISL) trunking.
5. Carrier Aggregation Switches — Carrier aggregation switches route traffic in addition to bridging (transmitted) Layer 2/Ethernet traffic that are designed for Ethernet networks that support video and high-bandwidth applications. Supports a variety of interface types, especially those commonly used by service providers.
6. Carrier Ethernet Access Switches – A carrier Ethernet access switch can connect directly to the customer or be utilized as a network interface on the service side to provide layer 2 services.
7. MPLS and Ethernet-Based WAN Solutions – Modern, scalable WAN technologies replacing legacy SONET networks.
8. Switch Features and Capabilities – the following list includes desired features and capabilities as necessary for the appropriate switch, as applicable:

    - Security Features: SSHv2 (Secure Shell Version 2), 802.1x (Port Based Network Access Control), Port Security, DHCP (Dynamic Host Configuration Protocol) Snooping, Two-Factor or Multi-Factor Authentication (2FA/MFA), MacSec encryption, Role-based access control lists (ACL)
    - Fast Ethernet/Gigabit Ethernet - 802.3bz (multi-gig interfaces 2.5Gbps and 5 Gbps)
    - 1/10/25/40/100/400 Gbps Support
    - PoE (Power over Ethernet) - up to 90/95W on all ports
    - Port Mirroring
    - Span Taps
    - Support of IPv6 and IPv4
    - Swappable powerlines and fans
    - AC or DC power supply minimum DC input ranging from 18V to 32 VDC and 36V to 72 VDC
    - Switch-port auto recovery
    - Dynamic Trunking Protocol (DTP)
    - Per-VLAN Rapid Spanning Tree (PVRST+)
    - IGP (Interior Gateway Protocol) routing, including non-proprietary such as IS-IS, OSPF, iBGP
    - EGP (Exterior Gateway Protocol) routing, including Border Gateway Protocol (BGP)
    - VPLS (Virtual Private LAN Service) Support
    - VRRP (Virtual Router Redundancy Protocol) Support

C. Networking: Storage

The emergence of new technologies creates an emphasis on storage devices that are connected via networks to servers to data to be accessed, managed, and shared efficiently across multiple systems. The goal is to provide managed centralized storage, increased scalability, and improved data protection and backup solutions.

This scope seeks various storage solutions that facilitate several use cases including, but not limited to, enterprise data centers, high performance computing, virtualization environments, artificial intelligence, security systems, backup and redundancy systems, and disaster recovery systems. Below is a list of storage solutions that are desired, this list is not limited to the storage devices or solutions that can be provided under this scope:

1. Storage Area Network (SAN): These devices are high-speed and specialize in block-level storage for data centers. This solution is protocol-independent and can be Fibre Channel (FC), FCOE or similar SAN topology for private cloud storage in virtualized environments.
2. Network Attached Storage (NAS): storage system at the file level connected to an IP network.
3. Fabric and Blade Server Switches: A Fibre Channel switch is a network switch compatible with the Fibre Channel (FC) protocol. It allows the creation of a Fibre Channel fabric, which is currently the core component of most SANs. The fabric is a network of Fibre Channel devices, which allows many-to-many communication, device name lookup, security, and redundancy. FC switches implement zoning; a mechanism that disables unwanted traffic between certain fabric nodes.

D. Optical Networking

High-capacity networks based on optical technology and components that provide routing, grooming, and restoration at the wavelength level as well as wavelength-based services.

1. Core DWDM (Dense Wavelength Division Multiplexing) Switches — Switches used in systems designed for long haul and ultra long-haul optical networking applications.
2. Edge Optical Switches — Provide entry points into the enterprise or service provider core networks.
3. Optical Network Management — Provides capabilities to manage the optical network and allows operators to execute end-to-end circuit creation.
4. IP over DWDM (IPoDWDM) — A device utilized to integrate IP Routers and Switches in the OTN (Optical Transport Network).

E. Wireless Networking

Wireless networking hardware are physical devices that enable data transmission without the use of physical cables, using radio waves, microwaves, or infrared signals to connect computers, mobile devices, and networks.

1. Wireless Access Points (WAP) – A device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. Capabilities should include:

    - 802.11a/b/g/n/ac/ and later
    - 2.4GHz, 5GHz, and 6GHz support
    - Should be capable of controller via DHCP, or automatically discovering cloud management system
    - Support for WPA2/WPA3
    - UL2043 plenum rated for safe mounting in a variety of indoor environments
    - Support AES-CCMP (128-bit)
    - Provides real-time wireless intrusion monitoring and detection

2. Wireless Router – Combination of a router and wireless access point, provides both internet access and Wi-Fi connectivity.

3. Outdoor Wireless Access Points – Outdoor APs are more rugged devices. Should be able to tolerate the elements of weather to tolerate a wide temperature range, high humidity, exposure to water, dust and oil, be able to be deployed virtually anywhere, provide real-time wireless intrusion monitoring and detection.

4. Wireless LAN Controllers — An onsite or offsite solution utilized to manage Light-weight access points in large quantities by the network administrator or network operations center. These devices are gateways that control user traffic aggregation. The WLAN controller automatically handles the configuration of wireless access points. Capabilities should include:

    - Ability to monitor and mitigate RF interference/self-heal
    - Support seamless roaming from AP to AP without requiring re-authentication
    - Support configurable access control lists to filter traffic and deny wireless peer to peer traffic
    - System encrypts all management layer traffic and passes it through a secure tunnel
    - Policy management of users and devices provides ability to de-authorize or deny devices without denying the credentials of the user, nor disrupting other AP traffic

5. Wireless LAN Network and Cloud-Based Services and Management — Enables network administrators to quickly plan, configure and deploy a wireless network, as well as provide additional WLAN services. Some examples include wireless security, asset tracking, and location services. Capabilities should include:

    - Provide for redundancy and automatic failover
    - Historical trend and real time performance reporting is supported
    - Management access to wireless network components is secured
    - RFC 1213 compliant
    - Automatically discover wireless network components
    - Capability to alert for outages and utilization threshold exceptions
    - Capability to support Apple's Bonjour Protocol / mDNS

- QoS / Application identification capability
- Zero-touch access point provisioning
- Network-wide visibility and control
- RF optimization,
- Firmware updates

6. Mobile Device Management (MDM) — MDM technology is utilized to allow employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and use those devices to access privileged government information and applications in a secure manner. Capabilities should include:

    - Ability to apply corporate policy to new devices accessing the network resources, whether wired or wireless
    - Provide user and devices authentication to the network
    - Provide secure remote access capability
    - Support 802.1x
    - Network optimization for performance, scalability, and user experience
    - BYOD/unmanaged device configuration (such as SecureW2 or CloudPath)

F. Security Hardware

1. Intrusion Detection/Protection and Firewall Appliances — Provide comprehensive inline network firewall security from worms, Trojans, spyware, key loggers, and other malware. This includes Next-Generation Firewalls (NGFW), which offer a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks.

    - Non-disruptive in-line bump-in-the-wire configuration
    - Network-address translation (NAT), stateful protocol inspection (SPI) and virtual private networking (VPN), etc.
    - Application awareness, full stack visibility and granular control
    - Capability to incorporate information from outside the firewall
    - Upgrade path to include future information feeds and security threats
    - SSL decryption to enable identifying undesirable encrypted applications (Optional)

2. Data Center and Virtualization Security Products and Appliances — Products designed to protect high-value data and data center resources with threat defense and policy control.

3. Application Delivery and Security – Includes application deliver controllers, load balancers, and Layer 7 Firewalls. Can be physical and virtual load balancers, WAFs, SSL offloading, and advanced traffic management.

III. DATA COMMUNICATIONS: SOFTWARE and CLOUD

Please note that software and cloud offerings are to be related to the functionality and solution-based data communications systems and solutions scope. It is recognized that advancements in technology have provided emerging solutions that do not require hardware or on-premises solutions to provide network and data communications capabilities. This Contract will not require software or cloud services to

be tied to a hardware purchase, however, the software and cloud offerings must strictly to relate to Data Communications as per the definition established in this Scope of Work.

Below is a list of software solutions, this list is not limited to the software solutions that can be provided under this scope:

A. Networking Software Solutions

Software covers a wide array of solutions required to support network operation and management within the scope of data communications. These consist of management tools to optimize area networks, or to ensure performance, optimization, capacity, data migration, data reduction and efficiency.

1. Networking Software – Software that runs on a server, or within the Cloud, and enables the server to manage data, users, groups, security, applications, and other networking functions. The network operating system is designed to allow transfer of data among multiple computers in a network, typically a local area network (LAN), a private network or to other networks. Networking software capabilities should include:

    - Restartable Process
    - High availability options
    - Targeted operating systems, i.e. DC, campus, core, WAN
    - Operating System Efficiencies
    - Network analysis tools (solutions utilized to collect, classify, analyze, and securely store log messages)
    - Load balancing – supports multiple balances in the same system, layer 4+7
    - Reporting
    - WAN optimization
    - Data compression
    - Network analysis tools (solutions utilized to collect, classify, analyze, and securely store log messages

2. Software Defined Networks (SDN) – Virtually manages flow control and can include SDN virtualized switches, routers, and controllers. These applications enable intelligent networking.

3. Automated Management Software for Network, Cloud, and Data Centers — Software products and solutions for network automation, cloud computing, and IT systems management to ensure secure, reliable, and scalable network operations.

    - Automate routine and repetitive tasks
    - Implement monitoring and alerting for proactive system maintenance
    - Provision, configure, and manage cloud resources (IaaS, PaaS, SaaS)
    - Automate backup, scaling, and deployment processes
    - Monitor server health, storage systems, and power usage
    - Ensure cloud security with identity management, encryption, and compliance controls

4. Edge Computing – Distributed processing near data sources to reduce AI and IoT applications.
5. DDI (DHCP, DNS, IPAM) Management Platforms – Integrated platforms for automating and securing core network services (DHCP, DNS, IP address management).

B. Security Solutions

Security of networks is paramount for the success of this scope of work and one of the most important aspects to ensure the confidentiality, integrity, and availability of data transmitted over communications networks. Security solutions will secure the data in transit across wired and wireless networks, prevent unauthorized access, inception, and tampering of communications. Security solutions will align with industry standards. The security solutions will enhance monitoring of the network. It is expected that networks be equipped with cutting edge security technology. Network systems need to be aware of the ever-changing landscape of threats, how to detect them, prevent them, and in cases where the threat is present, eliminate the threat.

Please note that this section refers to an array of desired security products. This does not supplement security requirements found in the Master Agreement Terms and Conditions. While some products may overlap or require additional negotiation with the Participating Entity, the MA security terms should be a baseline that take precedence and apply to all of the offerings.

Below is a list of security solutions, this list is not limited to the offerings that can be provided under this scope:

1. Network Security – These security measures will require a comprehensive solution that protect the network and digital infrastructure from cyber threats. These security measures include, but are not limited to:
    - Remote Browser Isolation (RBI): Keeps web content off endpoints to prevent drive-by downloads and malicious scripts.
    - Incident Response Solutions: Rapid-deployment networking solutions for emergency response, including drone communication hubs.
    - Zero Trust OT Security: Focused on securing operational technology environments with strict identity verification.
    - Zero Trust Network Access (ZTNA): Provides secure, identity-based access to applications regardless of location.
    - Malware Analysis & Sandboxing: Isolates and analyzes suspicious files or behavior in a secure environment before execution.
    - DNS Security: Blocks access to malicious domains and provides visibility into domain-level threats.
    - AI Access Security: Controls and monitors access to AI tools and platforms, helping prevent misuse or data leaks.
    - Data Center Security: Protects physical and virtual infrastructure in centralized or hybrid data centers.
    - Data Loss Prevention (DLP): Prevents sensitive data from being lost, leaked, or misused.

- Intrusion Detection and Prevention (IDPS): Monitors and blocks suspicious or malicious network activity.
- AI-Driven Network and Security Management - For automation, anomaly detection, predictive maintenance, and self-optimizing networks.
- IoT Security: Protects connected devices and their communication from exploitation.

2. Cloud Security – Consists of securing the communication channels, protocols, and endpoints involved in data exchanges across cloud services. These cloud security measures include, but are not limited to:

    - Cloud Secure Web Gateway: Protects users from malicious internet traffic, enforcing security policies in the cloud.
    - Cloud Access Security Broker (CASB): Bridges the gap between cloud service usage and enterprise security policies.
    - Cloud Security Posture Management: Continuously monitors and evaluates cloud configurations to ensure they meet security and compliance standards.
    - Cloud Workload Protection: Secures applications and services running in cloud environments by protecting workloads from vulnerabilities and threats.
    - Cloud Visibility, Compliance, & Governance: Provides centralized insight into cloud resources while enforcing policies for regulatory compliance and governance.
    - Secure Access Service Edge (SASE): Converges networking and security services into a single cloud-delivered platform.
    - Security Service Edge (SSE): Consolidates cloud-delivered security functions such as SWG, CASB, and ZTNA.
    - Cloud-Native Networking and Security: Tools and services supporting hybrid/multi-cloud deployments and modern security architecture.
    - Cloud Threat Detection: Identifies suspicious behavior, misconfigurations, and active threats across cloud environments using analytics and threat intelligence.
    - Infrastructure as Code (IaC) Security: Scans and secures infrastructure templates (e.g., Terraform, CloudFormation) to detect misconfigurations before deployment.

3. Identities and Access Management – Consists of managing user identities, controlling access to systems and data, and ensuring that access is granted based on the principle of least privilege. These management security measures include, but are not limited to:

    - Privileged Access Management (PAM): Secures, monitors, and controls access to critical systems by privileged users to reduce the risk of insider threats and credential abuse.
    - Identity as a Service (IDaaS): Delivers cloud-based identity management capabilities such as single sign-on (SSO), authentication, and user provisioning as a service.

- Access Management: Controls and enforces who can access what resources, when, and under what conditions, often integrating with authentication and authorization policies.
- Identity Governance and Administration (IGA): Provides policy-based controls to manage user identities, access rights, and lifecycle processes across the enterprise.
- Directory Services: Centralizes user identity data and authentication across systems, typically using technologies like LDAP, Active Directory, or cloud directories.
- Micro and Macro Segmentation Solutions: Granular (micro) and broad (macro) network segmentation for enhanced security and compliance.
- Identity Analytics: Uses data analysis and machine learning to detect anomalies, assess risks, and support access decisions in real-time.

C. Unified Communications – Integrated data communications solutions that can include hardware, software, and services.

Unified Communications (UC) is a solution that integrates multiple communications tools and technologies into a single cohesive end-user interface to enhance business communication. UC features include, but is not limited to the following:

1. Voice Calling (VoIP): Internet-based voice communication, includes E911 support.
    - Support for analog, digital, and IP endpoints
    - Flexibility to configure queue depth and hold time, play unique announcements and Music on Hold (MoH), log in and log out users from a queue and basic queue statistics
    - Enterprise Telephony Features (CFx, Transfer, CID, Shared line appearance, One Number Service, etc.)
2. Video Conferencing: Real-time video meetings and virtual collaboration.
3. Instant Messaging (Chat): Real-time text communication. Solutions that allow communication over the Internet Protocol, within the enterprise, and remotely, as well as with guest users that offers quick transmission of text-based messages from sender to receiver. In push mode between two or more people using personal computers, Desktop (Windows/Mac/VDI/Linux), Mobile/Smartphone, Tablet, along with shared clients, instant messaging basically offers real-time direct written language-based online chat. Instant messaging may also provide video calling, file sharing, PC-to-PC voice calling and PC-to-regular-phone calling
4. Email and Voicemail Integration: Unified inbox for different types of messages.
5. Presence Information: Shows user availability (e.g., available, busy, offline).
6. File Sharing & Collaboration Tools: Enables real-time co-editing and document sharing.
7. AI driven communication tools leveraging machine learning that automate and enhance communication experience and abilities.

D. Facilities Management, Monitoring and Control – Integrated data communications solutions that can include hardware, software, and services.

This integrated solution provides the capabilities of monitoring systems and control mechanisms to track, manage, and optimize building performance in areas such as energy, safety, HVAC, lighting, access, and IT infrastructure.

1. Monitoring – The use of technology such as sensors (hardware) and software to track building conditions and security. It can include environmental metrices, power usage, equipment usage and fault detection.
2. Control – The use of technology to automatically or manually manage and control systems in a physical space utilizing monitored data. It can include remote equipment operation, HVAC and lighting systems, power management and backup systems.
3. Security Systems – The use of data communications systems to provide video surveillance, facial recognition, thermal imaging, smart sensors, real-time alerts and forensic search. The employment of AI solutions that enable video surveillance and analytics is desired.

IV. DATA COMMUNICATIONS: SERVICES

This SOW seeks not only hardware and software offerings above, but a comprehensive service offering to ensure that all purchases of data communications hardware and software perform properly and optimally. The Contactor shall be responsible for the performance of all aspects of the contract, including the performance of all subcontractors.

A. Services and Consulting

To ensure success of data communications systems and networks, the SOW requires that the Contractor provide holistic solutions consisting of services including, but not limited to the following service areas:

1. Installation

- Site Survey and Assessment – Includes preinstallation site assessments to identify cabling paths, equipment locations, power requirements, and potential constraints
- Network Cabling and Physical Infrastructure – Installation of secured cabling systems and testing of all cables to ensure connectivity.
- Equipment Installation – Mount and install all hardware including firewalls, switches, routers, wireless access points, etc. Configure hardware to design and system specifications, including integrating power supplies.
- Wireless Network Deployment – Install and test wireless access points, optimize signal strength, secure access points by configuring encryption and protocols.
- Configuration and Integration – Load base configurations on hardware, integrate new hardware with existing systems.

- Testing and Validation – Includes performance testing, fault tolerance, connectivity and document results.

2. Maintenance

- Preventative Maintenance – Perform routine inspections and testing of data comm systems.
- Corrective Maintenance – Respond to system failures, cable faults, or connectivity issues. Replace faulty or defective components, restore service and limit downtime.
- Performance Monitoring – Monitor performance, analyze data traffic efficiency, identify congestion.
- System Configuration Management – Maintain backup copies of data comm system configurations, track and document changes to network.

3. Troubleshooting and Helpdesk

- Support Services – Provide Tier 1 (basic), Tier 2 (intermediate), and Tier 3 (advanced) support for data communication systems. Offer support in multiple channels (phone, email, chat, remote in)
- Incident Management – Log, categorize, prioritize, and track all incidents through a centralized ticketing system
- Guide users through troubleshooting steps for simple issues (e.g., cable checks, adapter settings)

4. Security

- Security Architecture and Design – Includes firewall and perimeter defense consulting.
- Updates and Patching – apply critical updates to system, test and update firewall rules, scan the system for network vulnerabilities.
- Data Encryption and Secure Transmission – Encrypt data in transit using protocols like TLS, IPSec, and VPNs. Secure communications between network nodes, cloud services, and remote users.

5. Training

- Conduct training and knowledge transfer sessions for Participating Entity staff and end users.
- Platforms for upskilling staff in AI, automation, network management, and cybersecurity.
- Provide user guides and quick-reference materials.

B. Service Level Considerations

This SOW seeks quality services administered with successful performance while recognizing that there are multiple potential Participating Entities with many different needs. This service level outline is meant to provide framework for the Contractor to incorporate as required and as appropriate per the service level agreed upon by the Contractor and Participating Entity.

1. **Performance Guidelines:**

    - Assign a contract manager to act as a liaison and contact person between the Purchasing Entities and the Contractor for the purpose of resolving issues or problems related to any part of this contract.
    - Follow the Participating Entities' state and local laws and regulations, especially labor and prevailing wage laws as well as all federal law (i.e. Davis-Bacon Act).
    - Employ skilled and experienced professionals for the specific task required to ensure highest quality and neat and expeditious performance.
    - Be licensed in each region, state, jurisdiction, etc. where Contractor is approved and awarded to work. Contractor or subcontractor performing work requiring a license must have obtained the license prior to commencing work. The Participating Entity reserves the right to reject a response if the responder fails to provide the Participating Entity adequate documentation of any required license. The Participating Entity reserves the right to verify any required license prior to final award and at any time during the work. The Contractor is responsible for the costs of obtaining or maintaining any licenses, permits, or other costs and shall not pass the cost through on an invoice.
    - Be responsible for obtaining all necessary permits, plan reviews, and inspections required for the work when applicable. Permits and Plan Reviews required by local authorities or the State shall be secured and paid for by the Contractor.
    - Provide all necessary payroll and prevailing wage reports along with any required statements of compliance along with their invoice.
    - Comply with each Participating Entity's cabling, electrical, and construction materials requirements.
    - Hazardous Materials – The Contractor is responsible for compliance with any Participating Entity requirements regarding hazardous materials. If the Contractor encounters a hazardous material or substance not addressed in the quote and if reasonable precautions will be inadequate to prevent foreseeable bodily injury or death to persons resulting from a material or substance, including but not limited to asbestos or polychlorinated biphenyl (PCB), encountered on the site by the Contractor, the Contractor shall, upon recognizing the condition, immediately stop work in the affected area and report the condition to the Participating Entity.
    - Final Acceptance of Completed Service by the Participating Entity – Upon completion of installation, maintenance, or repair services, Contractor must submit a request for written final acceptance of service completion from the Participating Entity. After receiving written final acceptance of completion of the service from the Participating Entity, the Contractor may issue an invoice to the Participating Entity. Contractor must satisfy all other Contract submittal requirements necessary for the service prior to submitting the request for written acceptance of service completion. If agreed upon by Participating Entity and Contractor, milestone payments are permitted. The milestones will be in writing and a part of the quote/contract between the Participating Entity and Contractor.

2. **Request for Quote**

- Provide a quote to any Purchasing/Participating Entity for data communications services and projects prior to any installation.
- Provide a not to exceed number of hours at the time of quote to complete the service and indicate whether the service will be performed on or off site.
- Provide the Participating Entity with a written quote of the amount of additional time needed to complete the service which the Participating Entity must approve in writing before continuing with the service, in the event the number of quoted not to exceed hours is met, but more time is needed to complete the service.
- Provide Contractor's name and subcontractor's name, and representatives.
- Date of quote and contract number at the top.
- Hardware, software, third party products information that will be used in the data communications solution – including price, extended pricing, quantity, license agreements, additional service level agreements.
- Estimated Quantity – clear and concise number of hours for all positions that will perform work.
- Any retainage information based on Participating Entity requirements.
- Any performance bond information based on Participating Entity requirements.
- Any additional fringe costs such as: milage, lodging, freight, as agreed upon with the Participating Entity.