2.1.1 Virtual Private Network Service [C.2.1.1]

MetTel proposes Virtual Private Network Service (VPNS) to provide secure, reliable transport of Agency applications across the MetTel core network. Our network is a national multi-service IP-enabled backbone that provides [redacted] VPNs are built across the MPLS core backbone between the Customer Edge (CE) router at the SDP connecting to the MetTel Provider Edge (PE) on the MetTel core network. Our VPNS provides both Secure and Trusted VPNs to build Intranets and Extranets and provide remote access.

MetTel VPNS

- Geographically diverse MPLS core network
- [redacted]
- Secure MPLS NNIs with national, regional, and global carriers
- FIPS 140-2 compliant devices with multiple encryption options

2.1.1.1 Compliance with Evaluation Criteria [L.29.2.1]

The MetTel VPNS solution fulfills the mandatory service requirements for VPNS in SOW paragraph C.2.1.1. This section presents a technical description of our offering and demonstrates our capabilities in Standards, Connectivity, Technical Capabilities, Features, Interfaces, Performance Metrics, and Security. **Exhibit 2.1.1-1** highlights some key strengths and benefits of our VPNS solution in relation to RFP Section M.2.1 evaluation criteria.

Exhibit 2.1.1-1. Features and Benefits of Approach to VPNS

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	[redacted] • Intranet, Extranet, and remote access using industry-standard protocols such as IPsec and TLS across properly sized access using various access means. • Secure VPNs that are based on IPSec, cryptographic algorithms, and industry-standard authentication methods and that transverse trusted VPNs or Internet Protocol Service (IPS) • Trusted VPNs that use the MetTel MPLS backbone and VRF definition to provide point-to-point, partial, and full meshed configurations.
Quality of Services (M.2.1(2))	• Full compliance with all SOW performance metrics including real-time and historic reporting of KPIs via the MetTel EIS Portal • 24x7x365 live customer support and service monitoring • Timely access to secure current and historic views of Agency network, trouble tickets, inventory, and billing

Evaluation Criteria	Features and Benefits of MetTel's Approach
	[redacted]
Service Coverage (M.2.1(3))	[redacted] • Global geographic coverage
Security (M.2.1(4))	• MetTel's network architecture ensures Agency's traffic is properly identified, routed (redirected), scanned (via DHS EINSTEIN enclaves), and delivered to the appropriate Agency network. Our architecture also enables us to identify any traffic that has been inadvertently directed through the EINSTEIN enclave and notify DHS. Metrics (SLA KPIs) are measured in accordance with the EIS RFP. • MetTel in partnership with Raytheon supports the standards defined for security and ensures Agency-specific requirements are met for identification and authentication, confidentiality, system and resource access control, security audit and logging, data and system integrity, continuity of service, security administration, and non-repudiation. • MetTel supports the proper safeguards for handling of VPNS traffic should failures occur with the DHS GFP. All DHS EINSTEIN enclaves are housed within a planned ANSI/TIA-942 and ICD 705 certified facility, located in northern Virginia.

2.1.1.1.1 Service and Functional Description [L.29.2.1, C.2.1.1.1, C.2.1.1.1.1]

The MetTel MPLS backbone is the core of VPNS and provides a secure, reliable transport supporting Agency applications such as voice, video, and data. [redacted] Agencies are able to securely support Intranets, Extranets, and remote access connections with cost-effective transport support for applications, voice, conferencing, and video using MetTel services.

MetTel's VPNS provides a reliable, secure network with extensive reach and access options. The MetTel MPLS network provides high-speed access across a wholly owned infrastructure housed in advanced telecommunications facilities. [redacted] **Exhibit 2.1.1-2** depicts the MetTel-deployed backbone.

Exhibit 2.1.1-2. MetTel MPLS Core VPNS Backbone

MetTel delivers our VPNS using our [redacted]. Our VPNS uses a private, dedicated infrastructure to establish RFC 4364 MPLS VPNs that enable large-scale deployments while minimizing the complexity usually associated with private lines and other VPN technologies. MPLS combines the performance and traffic management capabilities of Layer 2 switching with the scalability and flexibility of Layer 3 routing. MetTel separates customer traffic by VPN (defined by a VRF per RFC 4364 and RFC 4381 for VPN security), which results in a network that provides security equivalent to a Layer 2 network combined with scalability, advanced IP features, and fully meshed connectivity of a Layer 3 network. **Exhibit 2.1.1-3** shows an example of the flexible connection architecture of MetTel's VPNS with fully or partially meshed locations—each site with unique access methods and performance requirements.

[redacted] This standards-based

approach allows us to select the best partner for price and performance [redacted]

MetTel optimizes an Agency's applications using Class of Service (CoS) markings, which provide accurate and consistent transport with traffic prioritization and cost-effective use of network bandwidth. QoS on the MetTel VPNS supports prioritization of traffic for services such as voice, video and multi-casting, business-critical traffic such as voice and data, and non-critical traffic such as email.

The MetTel MPLS private network accommodates and optimizes an Agency's applications to ensure accurate and consistent prioritization of traffic. [redacted] **Exhibit 2.1.1-4** shows an example of how these classes can be defined to prioritize and control traffic across the MetTel VPNS.

[redacted]

Performance measurement and reporting are integral to the MetTel converged network. [redacted] **Exhibit 2.1.1-5** shows an example of the detail and real-time display of KPIs through the MetTel EIS Portal.

Exhibit 2.1.1-5. Link and Traffic Monitoring

Remote access VPNs use FIPS 140-2 compliant devices and clients to ensure security and functional requirements of the Task Order are met. Various remote connections are supported, including compliance with NIST 800-46 Rev. 1 for remote access/telework security. Connections can be Wi-Fi, wireless, broadband, and dedicated access to meet Agency requirements. Our high-speed IP-enabled backbone is standards-based and conforms to all EIS RFP requirements for the VPNS C.2.1.1.1. Functional Definition.

2.1.1.1.2 Standards [L.29.2.1, C.2.1.1.1.2]

Our VPNS supports all the standards defined in C.2.1.1.1.2 and provides trusted and secure VPNs. Trusted VPNs use the standard MPLS separation provided by Label Switched Paths (LSP) and VRF/BGP separation and routing. Secure VPNs are provided

by FIPS 140-2 compliant CE routers to provide the full suite of IPSec services, encryption algorithms, key exchange, and authentication services to support dedicated and remote access VPNs. Encryption algorithms include but are not limited to 3DES, RC4, AES 128, AES 256, IKEv1, and IKEv2. MetTel selects the compliant CPE and software based on specific requirements in the Task Order.

MetTel's VPNS is standards-based and supports both IPv4 and IPv6; either can be encapsulated in the other providing an effective strategy for transition to future services that may only be IPv6. The MetTel VPNS is an entirely private network enabling many customer requirements to be met using the RFC 1918 private address to define the Agency internal network and deliver the Agency publicly routable IP network for Internet-bound traffic and hosting.

MetTel complies with all standards defined in C.2.1.1.1.2 and will comply with new versions. We understand and comply with the evolving standards of these working groups to ensure the VPNS is compliant and provide quality services in a well understood framework. **Exhibit 2.1.1-6** provides a summary of the standards and how they are used in our VPNS.

Exhibit 2.1.1-6. Standards Utilization

2.1.1.1.3 Connectivity [L.29.2.1, C.2.1.1.1.3]

With the power and reach of the MetTel network, Government customer's locations and trusted business partners connect for site-to-site access or remote access to provide direct connectivity between all sites in a partially meshed or fully meshed Wide Area Network (WAN). We offer a wide variety of connection options and protocols that include Ethernet, traditional TDM, various speeds of private lines and SONET, DSL, cable, wireless, and satellite. Agency VPNs provide transparent access to Agency locations that use the MetTel EIS Ethernet Transport Service (ETS). We provide high-availability options for load sharing, failover protection, and diverse access to our POPs. MetTel meets all diversity requirements defined in C.2.9 and described in Section 2.1.5 for VPNS.

2.1.1.1.4 Technical Capabilities [L.29.2.1, C.2.1.1.1.4]

The MetTel network enables traffic to be identified by service for redirection to DHS EINSTEIN enclaves. Once processed, this traffic can be delivered to its final destination. We follow the DHS established procedures should any non-participating Agency traffic be sent through the DHS EINSTEIN enclave.

MetTel VPNS supports all the requirements of C.2.1.1.1.4. **Exhibit 2.1.1-7** defines the technical capabilities for security, and **Exhibit 2.1.1-8** provides the technical capabilities for connectivity and QoS.

Exhibit 2.1.1-7. Security Technical Capabilities Support

C.2.1.1.1.4 Reference	Feature	MetTel Response
1	Inspection	MetTel's network architecture ensures that Agency VPNS traffic is properly identified, routed (redirected), scanned (via DHS EINSTEIN enclaves), and delivered to the appropriate Agency network. Our architecture also enables us to identify any traffic that has been inadvertently directed through the EINSTEIN enclave and notify DHS. Metrics (SLA KPIs) are measured in accordance with the EIS RFP.
2	Tunneling Standards	MetTel provides a full suite of tunneling standards for security implementation. IPsec, MPLS, L2TP, GRE, IP-in-IP, and SSL/TLS for remote access are

C.2.1.1.1.4 Reference	Feature	MetTel Response
		implemented as required in a Task Order.
3	Encryption Algorithms	All encryption algorithms are implemented in accordance with FIPS 140-2 and other relevant FIPS publications and modules. Encryption algorithms include but are not limited to 3DES, RC4, and AES 128 and AES 256.
4	Authentication	MetTel supports a variety of customer, third-party, and internal authentication mechanisms. These include but are not limited to RADIUS, Internal LDAP, tokens, PKI, and X.509 certificates depending on the Agency requirements specified in the Task Order.
10	Isolation and Layering	[redacted] Using physical separation of routers and standard VLAN and MPLS and VRF technology, the MetTel VPNS is layered such that any single point of entry requires traversing multiple secured layers.
12	Secure Routing	[redacted]
13	Security Management	MetTel provides encryption, decryption, and key management profiles as part of the security management system to meet specific requirements as specified in an Agency Task Order.
14	Agency Mechanisms	MetTel supports the inclusion of Agency-deployed internal security mechanisms.
15	Authentication of Temporary Access users	Mechanisms for authentication of temporary access users are provided on servers that are contractor-, Agency-, or third-party provided.

Exhibit 2.1.1-8. Connectivity and Quality of Service Technical Capabilities Support

C.2.1.1.1.4 Reference	Feature	MetTel Response
5	IPv4 Support	MetTel supports IPv4 as both the encapsulating and encapsulated protocol.
6	IPv6 Support	MetTel supports IPv6 as both the encapsulating and encapsulated protocol.
7	QoS Modes	MetTel supports QoS in the multiple standardized modes, including Best effort, Aggregate CE interface (“hose” level), site-to-site level (“pipe” level), Intserv (RSVP) signaled, and Diffserv marked.
8	QoS on Access	MetTel supports QoS across a subset of the AA networks including 802.1p Prioritized Ethernet, MPLS-based access, Multilink Multiclass PPP, and QoS-enabled Wireless for LTE, Wireless 802.11.x. Also supported are cable high-speed access (DOCSIS 1.1), QoS-enabled Digital Subscriber Line (DSL) and QoS-enabled Satellite Broad Band Access. QoS availability is dependent on location and carrier support for the specified QoS and the requirements of the Agency Task Order.
9	Application-level QoS	MetTel supports the following application-level QoS objectives: the Intserv model for selected individual flows and the Diffserv model for aggregated flows.
11	Multiple VPNs	MetTel supports multiple VPNs by allowing permanent and temporary access to one or more VPNs for authenticated users across a broad range of AAs.

2.1.1.1.5 Features [L.29.2.1, C.2.1.1.2]

High Availability Options

MetTel provides high-availability options for VPNS using the AAs as defined in Section 2.1.5 and Service Related Equipment (SRE) configured to provide load sharing, failover protection, and diverse access points to MetTel POP(s). The following sections describe our approach to providing the required high-availability options.

1. Load Sharing

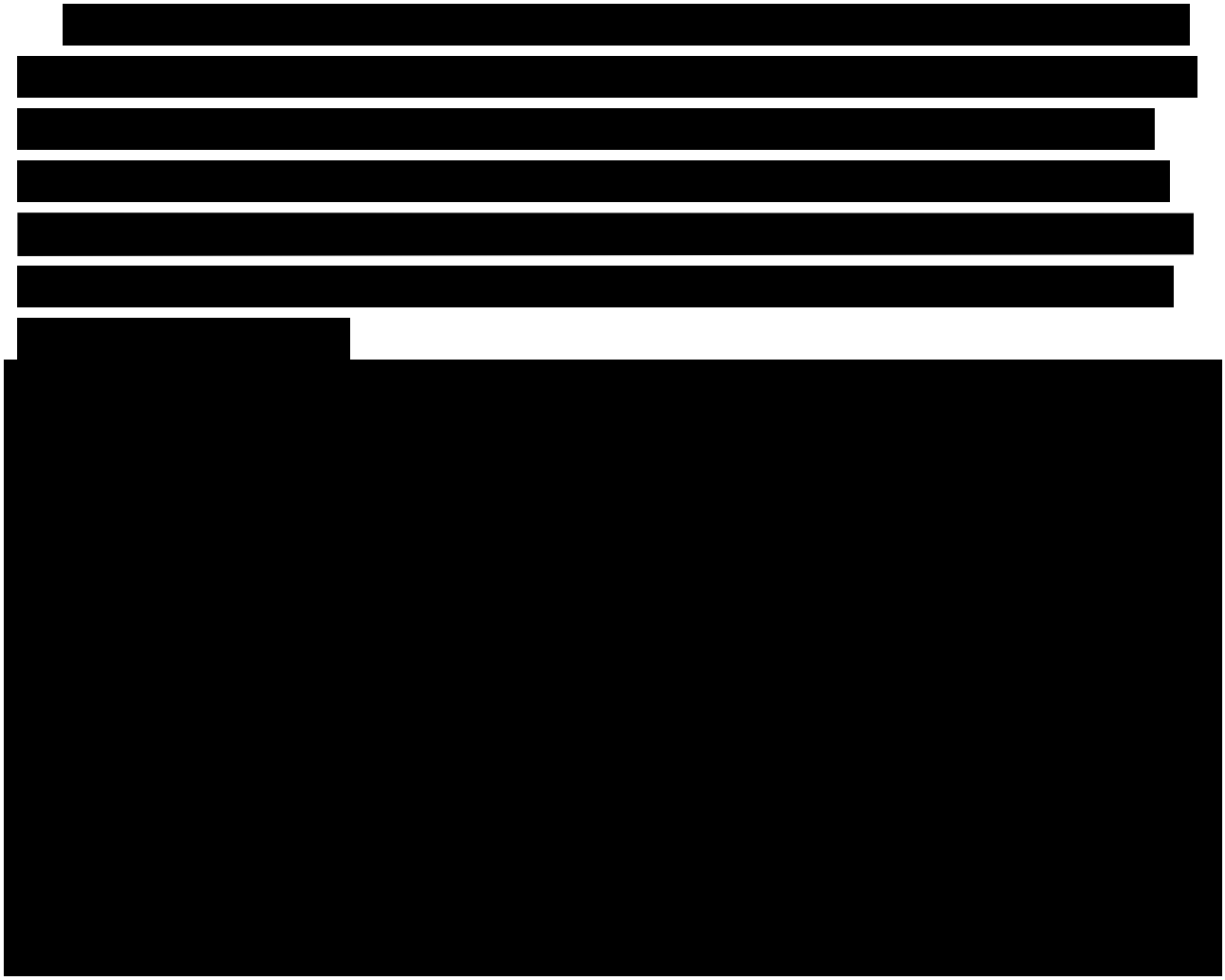

Exhibit 2.1.1-9. Load Sharing Configurations for VPNS

2. Failover Protection

Failover protection is provided using two circuits to the MetTel network and two SREs. Routing protocols such as BGP and EIGRP weigh the two connections and

choose the available primary or high route and switch to the alternate on failure. Several options, depending on customer requirements, are available for weighting criteria such as round robin or calculated load. When the high path becomes operational, routing resumes using the highly weighted path. Failover protection is enhanced with the second or alternate circuit connected to a second MetTel POP. **Exhibit 2.1.1-10** provides an example of failover protection showing redundant connections to a single POP or optional redundancy to multiple geographically diverse POPs.

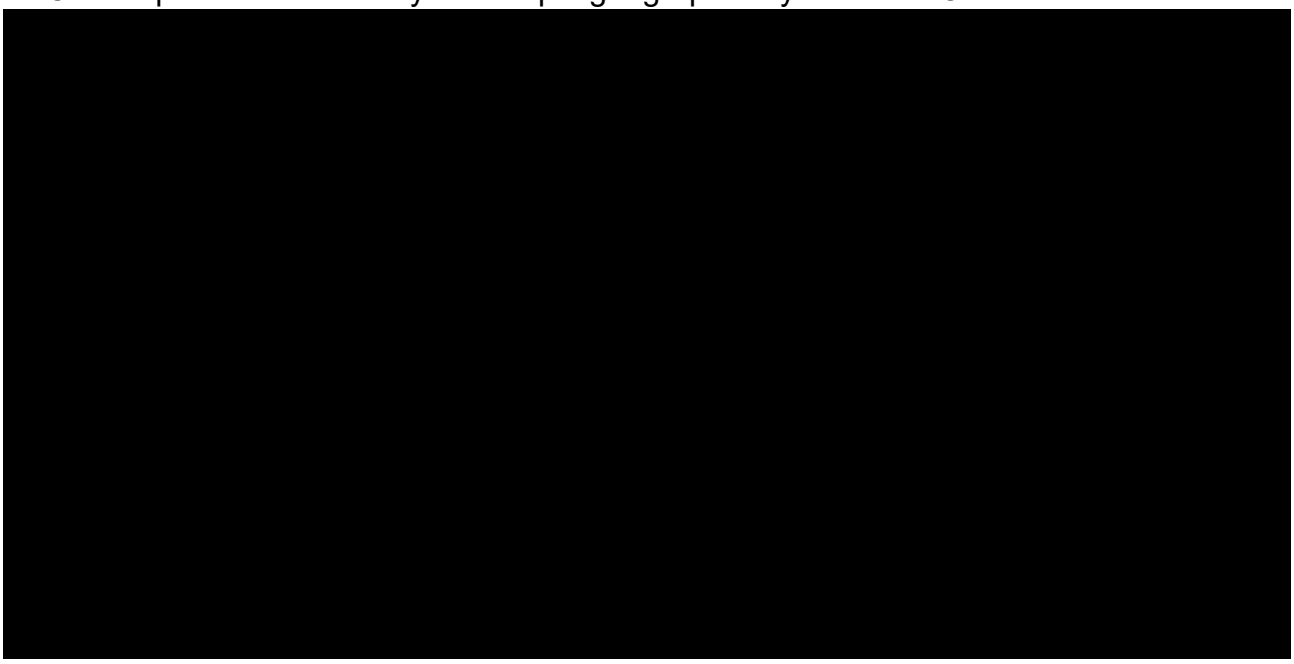

Exhibit 2.1.1-10. Failover Configurations for VPNS

3. Diverse Access Points to MetTel POPs

Diverse access points to MetTel POPs are used in implementation of failover and provide separate physical paths to the MetTel POPs. Circuits can be run to separate PE routers in the same POP or to physically separate POPs. Routing mechanisms such as BGP or EIGRP are used to select the alternate path if the primary path is not available. **Exhibit 2.1.1-11** shows sample configurations for both types of diverse access to MetTel POPs.

Exhibit 2.1.1-11. Diverse Access Points to MetTel POPs for VPNS

2.1.1.1.6 Interfaces [L.29.2.1, C.2.1.1.3]

The SRE for VPNS provide all the mandatory UNIs defined in RFP C.2.1.1.3.

2.1.1.1.7 Performance Metrics [L.29.2.1, C.2.1.1.4]

Our embedded performance collection and management capabilities provide real-time and historic reporting of the Acceptable Quality Levels (AQL) of KPIs for the VPNS. [redacted] maintains and reports latency and availability via the Management and Maintenance element of the MetTel EIS Portal, and the Trouble Ticketing element of the MetTel EIS Portal maintains and reports time-to-restore.