

2.3 External Traffic Routing Requirement [L.29.2.3, C.1.8.8]

Understanding

MetTel acknowledges and fully understands that EIS is a key component of the U.S. national telecommunications infrastructure and that GSA will provide Government users with services and service elements (technical, management, and operations related) that are acquired through EIS and in compliance with national policy directives that apply to the national telecommunications infrastructure.

We acknowledge and fully understand that specific national policies include, but are not limited to:

1. NS/EP requirements that include a wide range of Executive Orders and 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.
2. OMB Memorandum M-05-22 that directs Agencies to transition from IPv4 Agency infrastructures to IPv6 Agency infrastructures (network backbones). Our solution(s) maintain functionality for Agencies with an IPv6 network (and those implementing IPv6 networks) with IPv4 legacy support, and we comply with NIST SP 500-276. All systems, software, and equipment supporting the Participating Agency network and its services handle IPv6 in an equivalent or more improved way than current IPv4 capabilities, performance, and security. We will not deploy systems, software, and/or equipment in support of the EIS that does not meet the IPv6 requirement. All network management within the A&A boundary for the EIS will be enabled for IPv6.
3. OMB Memorandum M-09-32 "Update on Trusted Internet Connections Initiative." We will exercise full due diligence in successfully integrating the National Cyber Protection System (EINSTEIN) deployments, effectively synchronizing with US-CERT and OMB Memorandum M15-01. Any of our service offerings under EIS, such as [REDACTED]

External Traffic Routing Highlights

- MetTel has fully functioning NS/EP capabilities
- MetTel fully supports IPv6 and IPv4
- MetTel will identify and route VPNS, ETS and IPS traffic traversing the public internet, extranet, and/or Inter-Agency Government traffic through MTIPS and DHS EINSTEIN Enclaves
- MetTel provides geographically diverse connections to Participating Agencies
- End-to-end Participating Agency traffic isolation and aggregation

[REDACTED] and/or Inter-Agency Government traffic will be identified and routed through a secure latest-generation Managed Trusted Internet Protocol Services (MTIPS) and DHS EINSTEIN Enclaves for processing. We will design, implement, and operate our services to achieve the required routing of Government traffic (including delivery to and receipt from) through MTIPS and DHS EINSTEIN Enclaves, which are strictly intermediate hops and not considered end points. KPI SLA measurement and transport SLA KPIs are measured as if through loopbacks in MTIPS and EINSTEIN Enclaves.

If contract modifications are required to meet new Government-specific requirements, we will submit a technical approach and schedule for proposing these new requirements to the CO as defined in § J.4.

2.3.1 Methodology for Identifying Agency Traffic [L.29.2.3 (1)]

To meet the External Traffic Routing requirements, the MetTel Team will build the MTIPS Portals [REDACTED]

[REDACTED] for inspection prior to delivery to destination. In the event an agency has bifurcated its data network and MTIPS, the routing discussed below will still apply.

[REDACTED]

The BGP announces routes from the router at the Participating Agency's SDP to the [REDACTED]. In the event the [REDACTED] is supplied by MetTel and becomes unavailable for any reason, the BGP session announces the Participating Agency's routes to the [REDACTED]. We determine [REDACTED] [REDACTED] for the Participating Agency based on [REDACTED]

Our external routing solution provides defense in layers by [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] At the top layer, Internet access routers provide connectivity to and from the Internet. [REDACTED]

[REDACTED]

[REDACTED]

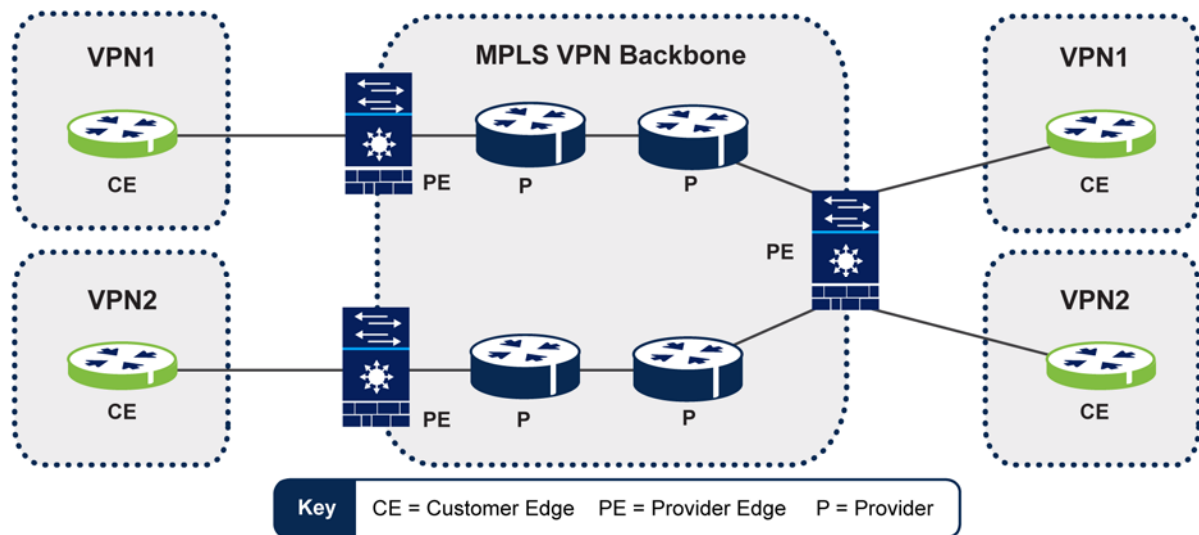
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Exhibit 2.3-1 illustrates the three roles a device can play when deploying MPLS.



MET_EIS_111v04

1. Customer Edge (CE) Router – Traditionally the network device at the customer location that interfaces with the service provider. The CE1 and CE2 represent the routers at the customer remote locations that need to be interconnected via the MPLS service provider network.
2. Provider Edge (PE) Router – The device at the edge of the service provider network that interfaces with the customer devices. They sit at the edge of the MPLS-enabled network and are often also called Label Switching Routers Edge (LSR-Edge).
3. Provider (P) Router – The devices building the core of the MPLS-enabled network. Their main function is to label switch traffic based on the most external MPLS tag imposed to each packet and are often called Label Switching Routers (LSRs)

Exhibit 2.3-1. MPLS Device Roles

[REDACTED]

[REDACTED]

[REDACTED]

This solution offers the combination of the industry's most [REDACTED] with a comprehensive range of next-generation network security services, including:

- Granular visibility and control
- Robust web security
- Industry-leading Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to protect against known threats
- Comprehensive protection from threats and advanced malware
- Virtualization of firewalls to provide separate traffic specific policies
- High availability for high-resiliency applications

[REDACTED]

[REDACTED]

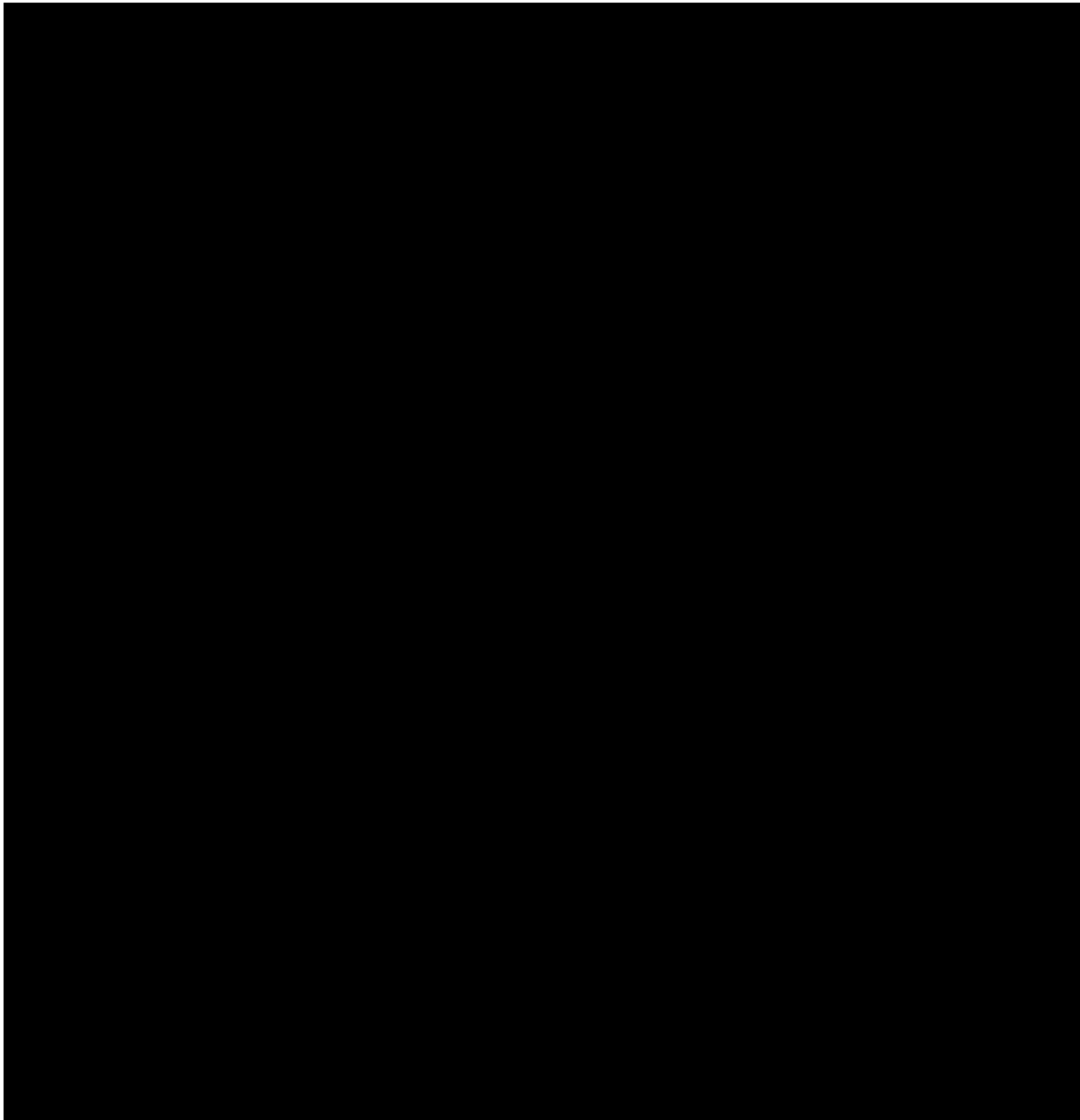
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



2.3.2 Approach to Redirecting Agency Traffic to EINSTEIN [L.29.2.3 (2)]

The MetTel architecture allows agencies to interconnect their networks transparently over the [REDACTED]. MetTel delivers connections to agency sites in the Continental U.S. (CONUS) Outside the Continental U.S. (OCONUS) and has international capabilities. [REDACTED]



[REDACTED] MetTel provides geographically diverse connections to provide added reliability. [REDACTED]

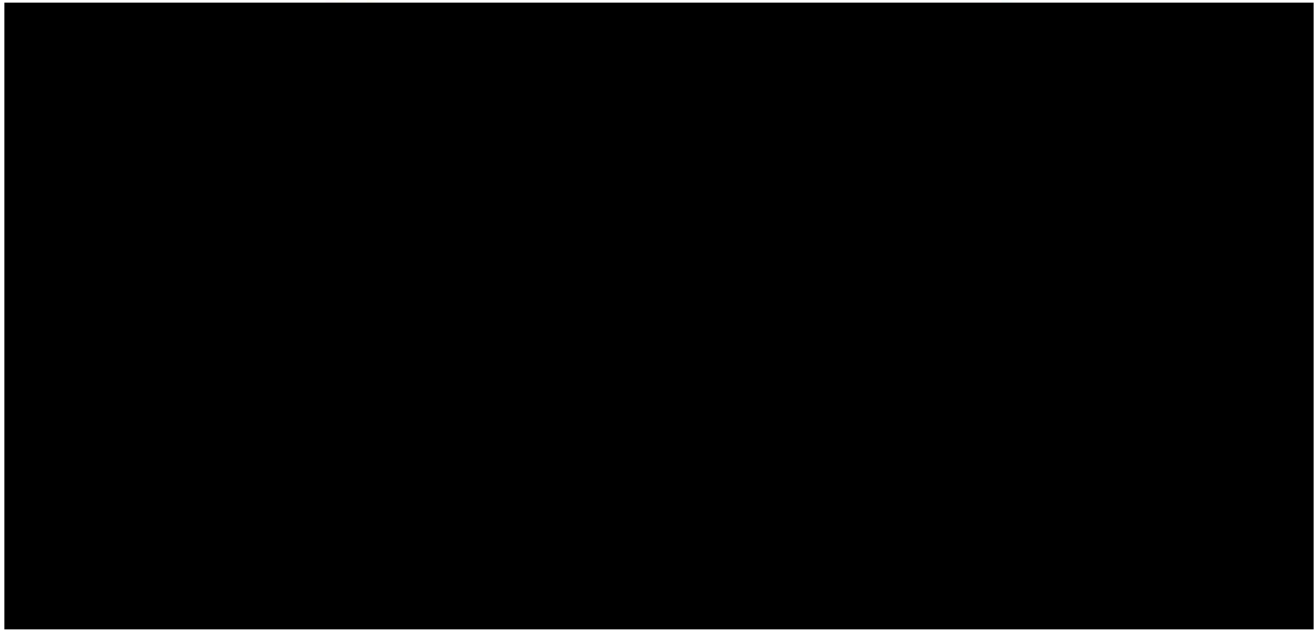
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED], MetTel provides the most cost-effective network reach to all domestic CBSAs. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]



[Redacted]

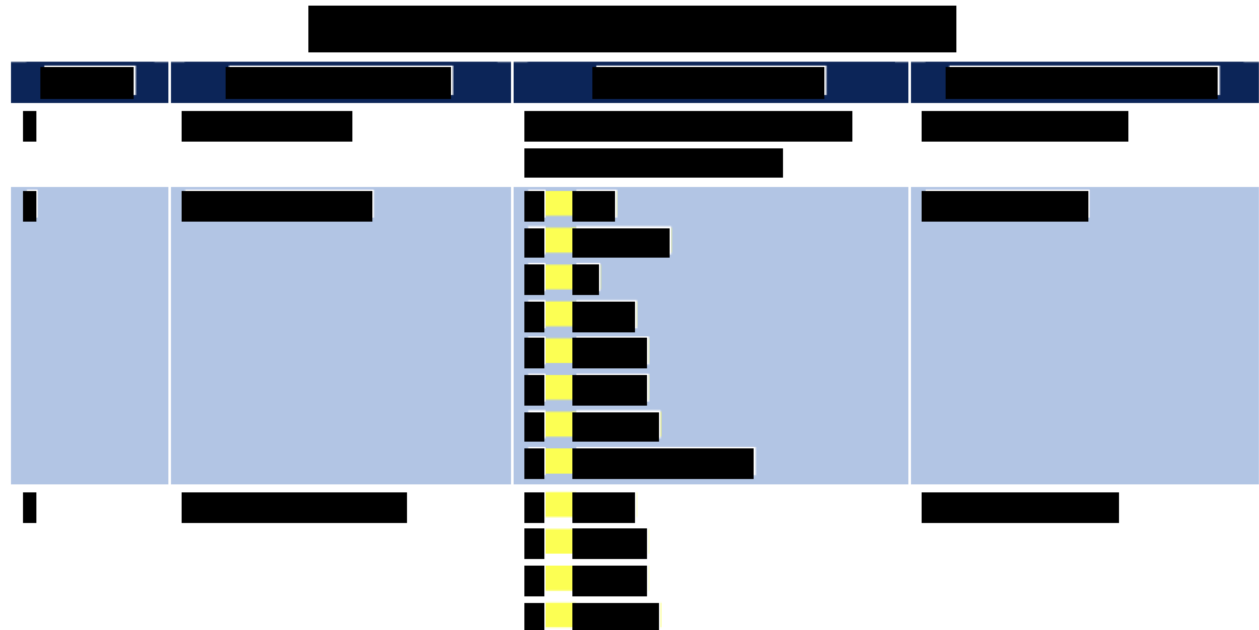
[Redacted]

[Redacted] This architecture is a network that provides any service to any EIS location, including mandatory services to all Government locations within all 100 top CBSAs and 812 additional CBSAs.

[Redacted]

[Redacted]

[Redacted]



[Redacted text block containing multiple lines of blacked-out content]

[Redacted header text]

[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]

The MetTel [REDACTED] network is the foundation for EIS services. MetTel has recently deployed the next generation infrastructure that takes the core network to new levels of flexibility and traffic delivery by leveraging [REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

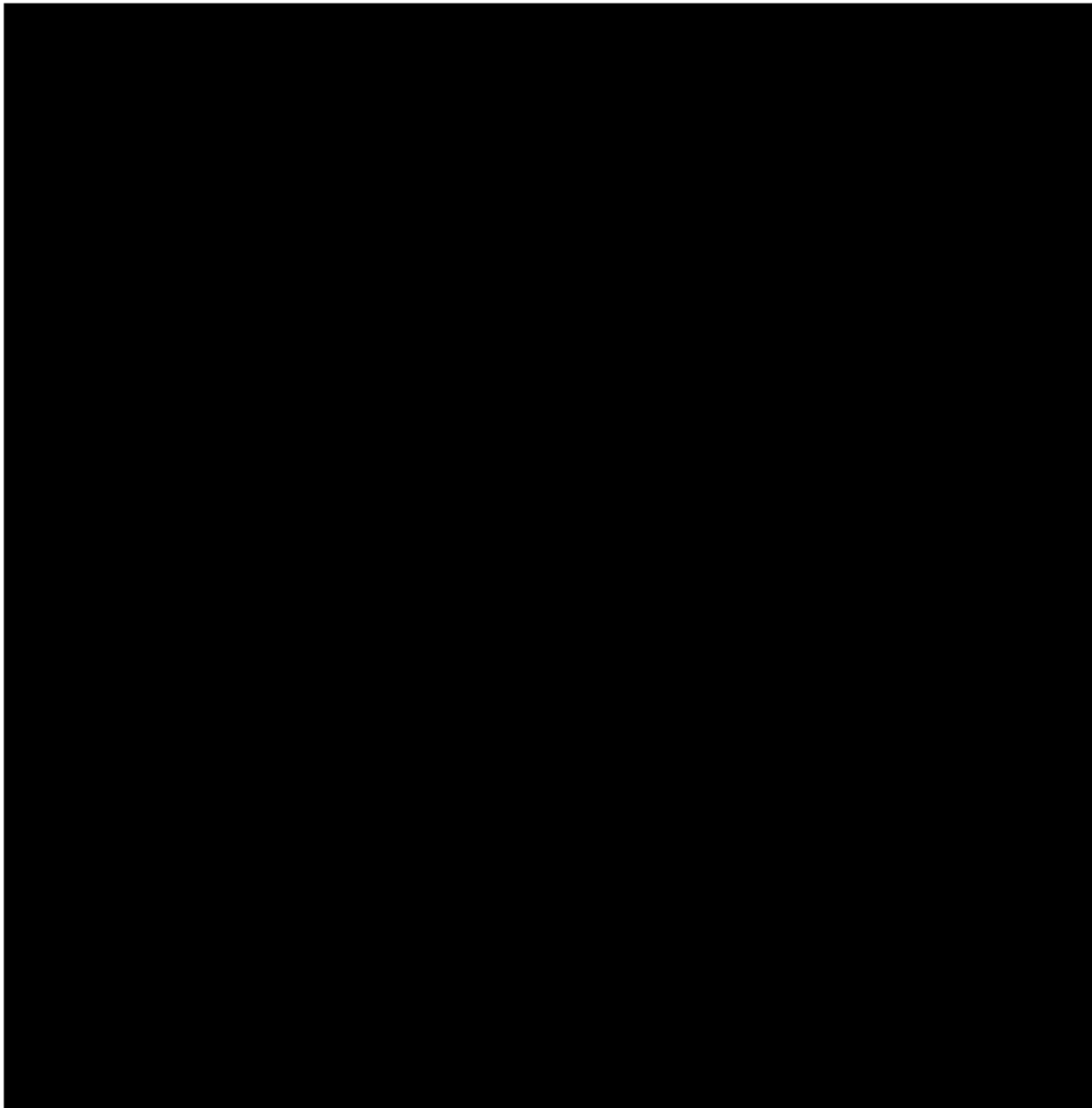
[REDACTED]

Our remote access point supports telework/remote access for authorized staff and users using VPNs through external connections, including the Internet. [REDACTED]

[REDACTED]

We support a variety of customer, third-party, and internal authentication mechanisms including but not limited to RADIUS, Internal LDAP, tokens, PKI, and X.509 certificates depending on the Participating Agency's requirements specified in the Task Order.

[REDACTED]



[Redacted text block consisting of multiple horizontal black bars]

[REDACTED]


[REDACTED] VPN access point supports dedicated external connections to external partners and business partners as well as MetTel MPLS connected Participating Agencies. [REDACTED]

[REDACTED]

[REDACTED] The following baseline capabilities are supported for external dedicated VPN and private line connections at the VPN Access Point:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

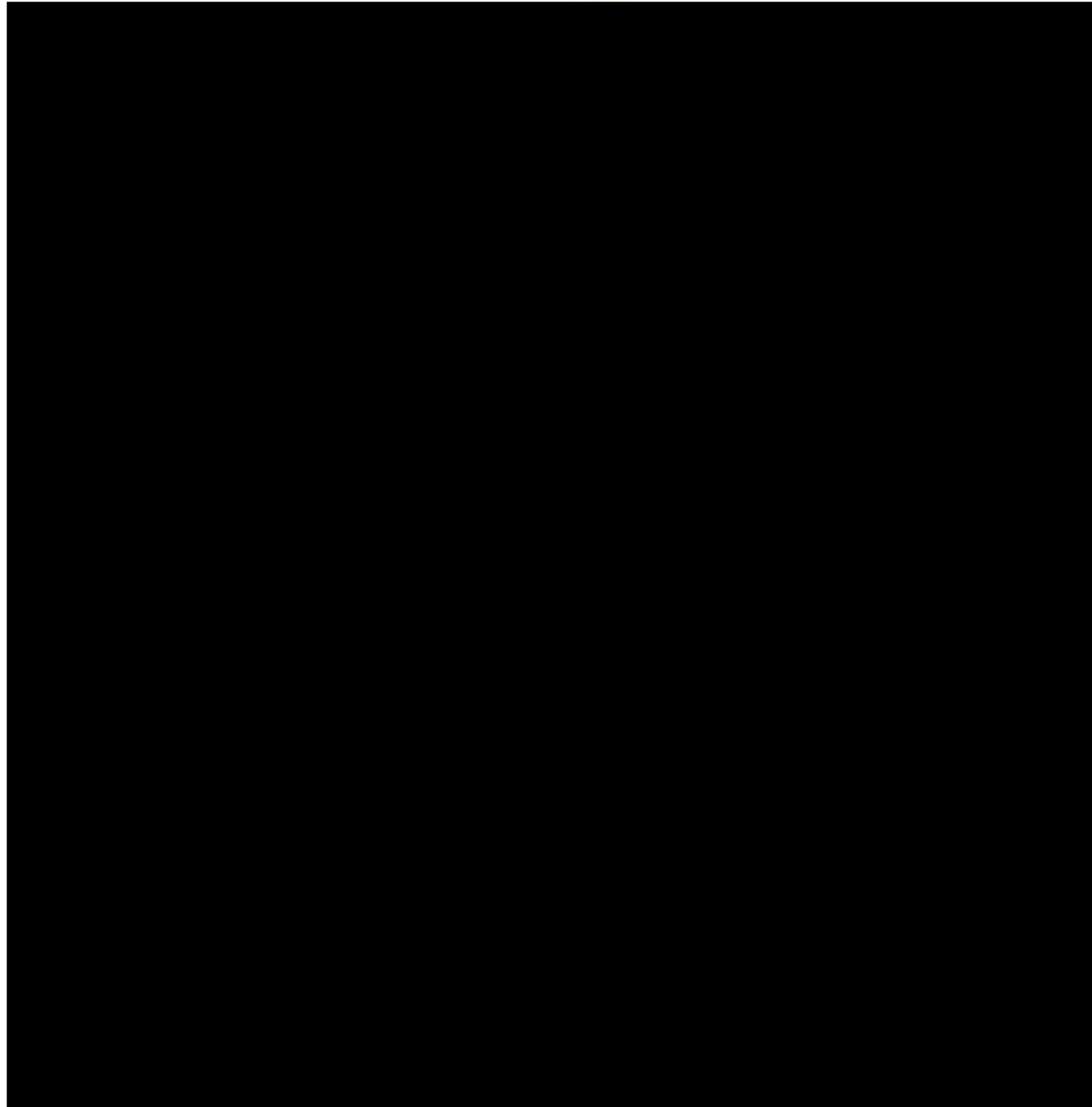


Our Extranet access point supports dedicated Extranet connections to internal partners. 

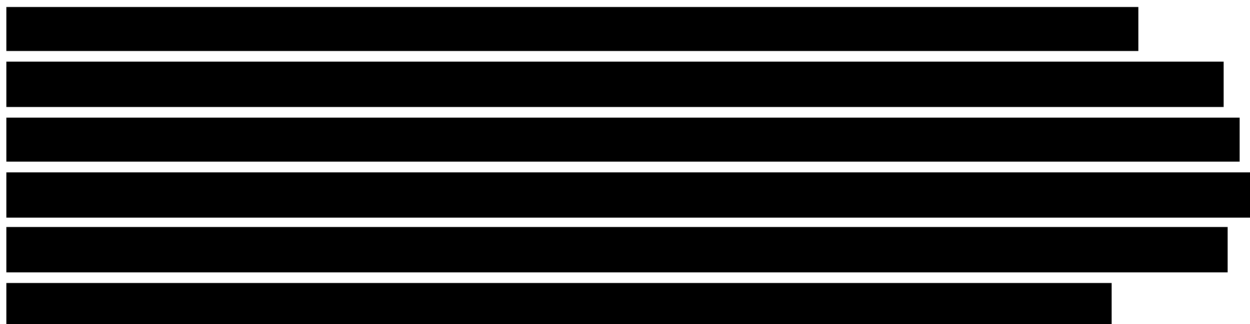


[Redacted text block containing multiple lines of blacked-out content]

routing.



If the Participating Agency's MTIPS Portal is hosted by another MPLS vendor,



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.3.3 Approach to Notify DHS of Non-Participating Agency Traffic [L.29.2.3 (3)]

Our [REDACTED] network is a highly reliable solution. [REDACTED]

[REDACTED] Agencies benefit from high-quality

[REDACTED]

System monitoring provides operators real-time analysis of individual device health and behaviors. [REDACTED]

[REDACTED]

This awareness is critical in making decisions during an attack or service outage. Therefore, the monitoring system provides access to audit compliance capabilities along with fallback tools in the event of misconfiguration. [REDACTED]

[REDACTED]

[REDACTED] This strategy provides safeguards needed to maximize network uptime and minimize threat impact.

2.3.6 Location of Certified Facilities [L.29.2.3 (6)]

The Primary DHS EINSTEIN Enclave will reside at the DHS Certified SCIF at the [REDACTED] Other sites will be selected in the future based on best locations to provide geographic diversity, high availability and best end-to-end performance for Participating Agency locations.

2.3.7 Availability of TS/SCI-Cleared Personnel [L.29.2.3 (7)]

The MetTel Team employs trained, qualified, and cleared staff (U.S. citizens) to support network design, configuration, and operation functions 24x7x365. The MetTel NOCs are staffed with personnel with appropriate credentials to manage technical aspects of the network. We perform enhanced background examinations of our staff members and follow the Federal background investigation protocol specified in the EIS RFP.

The MetTel Team applies the principal of role-based access so that only those MetTel staff with a verified need for access to our network infrastructure are granted

access. In addition to role-based access, every MetTel Team user has individually, specifically assigned access rights and privileges that apply the principal of “least access.” [REDACTED]

[REDACTED]

All user access logs are retained in full compliance with the EIS RFP. [REDACTED]

[REDACTED]

2.3.8 Instrumentation to Measure Transport KPIs [L.29.2.3 (8)]

Our embedded performance collection and management capabilities provide real-time and historic reporting of the AQL of KPIs for the [REDACTED]

[REDACTED]