2.1.11 Managed Trusted Internet Protocol Service [C.2.8.4]

The MetTel Managed Trusted Internet Protocol Service (MTIPS) architecture is built by industry leading security professionals from MetTel teammate Raytheon. Participating Agencies (PAs) will be secured through this architecture by having its traffic inspected at many levels, ensuring protection.

MetTel MTIPS

- Architected to enable the industry's best security
- Scales rapidly to meet Agencies' growing needs
- High availability through redundant failover systems
- Easily expandable to IPSS capabilities

[redacted].

Network forensics is provided through packet capture devices, which can produce a file of the traffic that has passed through the MTIPS system. After the MTIPS system inspects the traffic, it is passed back [redacted]

[redacted]

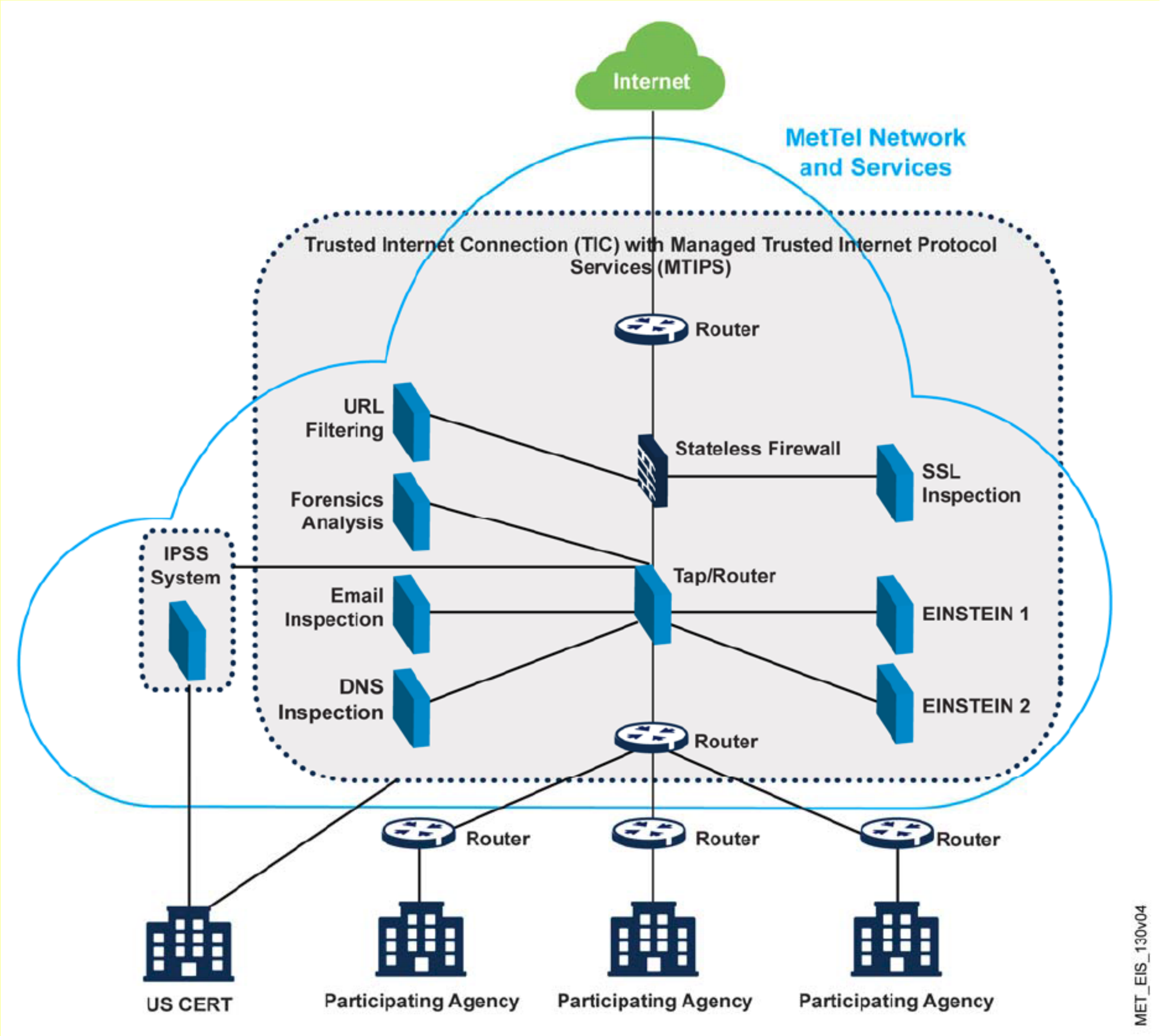

Exhibit 2.1.11-1 MTIPS Configuration and High Level Data Flow

2.1.11.1 Compliance with Evaluation Criteria [L.29.2.1]

The MetTel MTIPS architecture meets the mandatory service requirements in SOW paragraph C.2.8.4. This section presents a technical description of the offering, demonstrating the capabilities in Standards, Connectivity, Technical Capabilities, Features, Interfaces, Performance Metrics, and Security. **Exhibit 2.1.11-2** highlights some key strengths and benefits of the MTIPS solution in relation to RFP evaluation criteria.

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

Exhibit 2.1.11-2. Features and Benefits of MetTel MTIPS Architecture

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• Network and System Architecture meets or exceeds all requirements for the TIC and MTIPS instantiations as specified by DHS • Provides stateless firewall, URL filtering, e-mail and DNS security, packet capture, SSL inspection, and connectivity to the GFE EINSTEIN appliances. • Equipment monitoring provided by MetTel Network Operations Center (NOC) • Equipment security monitored by MetTel teammate Raytheon Security Operations Center (SOC) • MetTel Network Architecture was built with the redundancy and reliability required for Internet access to mission critical needs
Quality of Services (M.2.1(2))	• Each MTIPS node is architected to implement all security, redundancy, failover and performance requirements. [redacted]
Service Coverage (M.2.1(3))	[redacted]
Security (M.2.1(4))	• Equipment monitoring provided by MetTel Network Operations Center (NOC) • Equipment security monitored by MetTel teammate Raytheon Security Operations • MTIPS locked down according to the MTIPS Risk Management Framework [redacted] • Enables the identify of any traffic that has been inadvertently directed through the DHS EINSTEIN Enclave and notifies DHS • Supports the proper safeguards for handling traffic should failures occur with the DHS GFP • DHS EINSTEIN enclave are housed within a separate caged area • IPSS planned in a ANSI/TIA-942 and ICD 705 certified facility

2.1.11.1.1 Service and Functional Description [L.29.2.1, C.2.8.4.1, C.2.8.4.1.1]

The MTIPS is a key component of the US national telecommunications infrastructure. As such, the General Services Administration (GSA) expects to effectively provide assurance for government users that the services and service elements (technical, management and operations related) acquired through EIS are in compliance with national policy directives that apply to the national telecommunications infrastructure.

The EIS service offerings transporting the public Internet, Extranet and/or Inter-Agency government traffic, will be identified and routed appropriately, either directly or through the MTIPS architecture. The MTIPS architecture includes firewalls, DNS security, e-mail security and the DHS EINSTEIN enclave devices. Encrypted traffic is also decrypted and inspected by this suite of devices via certificate loading at the PA's.

[redacted]

Any additional policy or standards required by the PA will be made part of the contract so that the PA continues to perform to the standards and remains compliant. MetTel will submit a technical approach and schedule for proposing these new requirements to the CO as per the contract modification guidelines identified in EIS RFP Section J.4.

GSA and the Department of Homeland Security (DHS) jointly developed the requirements for the EIS Trusted Internet Connection Access Provider (TICAP) service. The high-level functional components include:

- Redundant Internet access
- Hosted EINSTEIN enclaves
- A Security Operations Center (SOC)
- MTIPS transport and services

MetTel and Raytheon have teamed to provide an ICD 705 compliant Sensitive Compartmented Information Facility (SCIF) for harboring and processing classified material.

The TIC architecture provides a PA centralized secure Internet access point that an entire PA can use from any of the Core Based Statistical Area (CBSA) locations. The MTIPS solution provides security services on top of the TIC solution to the PA's. This allows the PAs to comply with OMB guidance on Trusted Internet Connections. The services include an EINSTEIN enclave providing customized threat mitigation, analytics, and network flow capabilities; e-mail inspection; encrypted traffic analysis; URL filtering; firewall protection; and DNS filtering for the PA's Internet connection traffic.

The MTIPS Security Operations Center (SOC) monitors all of the equipment to proactively detect malicious activity and remediate threats that are found. Additionally, this service is available to the PAs for monitoring their alerts by Raytheon Foreground Security.

It is understood that the MTIPS system is subject to periodic DHS Cybersecurity Compliance Validation (CCV). DHS is responsible for the “Compliance and Assurance Program (CAP)”. The CAP employs a collaborative approach and measures, monitors and validates the implementation of cross-government initiatives and assesses cyber risks. Under CAP, the MTIPS subscriber agencies shall complete an annual Cybersecurity Compliance Validation (CCV) self-assessment and DHS will conduct an on-site CCV every three years. MetTel, as a MTIPS contractor, will participate in an annual DHS led CCV assessment.

The MTIPS instantiation that the MetTel team is offering is fully compliant with the DHS MTIPS requirements. Each node is architected with security, redundancy, failover and performance in mind. Multi-site redundancy allows the MTIPS enclave to provide continuous operations, even with regional disruptions. [redacted] performance is continuously monitored by the MetTel NOC to ensure that Service Level Agreements with the PAs are being maintained and reported.

2.1.11.1.2 Standards [L.29.2.1, C.2.8.4.1.2]

The MetTel team will comply with all the current and future regulations, policies, requirements, standards, and guidelines for Federal U.S. Government technology and cyber security and within 90 days of EIS award, will deliver a plan for adoption of applicable standards. The MetTel team will submit an updated plan to the CO within 90 days of issuance of new TIC/MTIPS capabilities or policy changes. MetTel will respond to new document versions, amendments, and modifications which may include minimum expectations for identified MTIPS-specified security services.

Specific national policies include, but are not limited to:

- 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.

- OMB Memorandum M-05-22 which 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) with IPv4 legacy support, the MetTel solution(s) will maintain functionality and fully understand and will comply with NIST SP 500-276. MetTel acknowledges and fully understands that all systems, software and equipment supporting the Participating Agency network and its services will handle IPv6 in an equivalent or improved way than current IPv4 capabilities, performance and security. MetTel acknowledges and fully understands not to deploy systems, software and/or equipment in support of the EIS which does not meet the IPv6 requirement. MetTel further acknowledges and fully understands that all network management within the A&A boundary for the EIS will be enabled for IPv6.
- OMB Memorandum M-09-32 “Update on Trusted Internet Connections Initiative” and 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.
- Office of Management and Budget’s (OMB) Trusted Internet Connections (TIC) initiative (M-08-05).

2.1.11.1.3 Connectivity [L.29.2.1, C.2.8.4.1.3]

The MetTel team’s MTIPS connects and interoperates with the following:

- The Public Internet
- EINSTEIN Enclave
- Global Response Loop to US-CERT with a cross-agency view that allows for coordination across TIC Portals.
- Rapid Response Loop from DHS to agency communications for the dissemination of threat/events to/from the Agency.
- Other Agency IP networks via External or Internal connections

2.1.11.1.4 Technical Capabilities [L.29.2.1, C.2.8.4.1.4]

2.1.11.1.4.1 TIC Portal Capabilities [L.29.2.1, C.2.8.4.1.4.1]

Exhibit 2.1.11-3 provides the TIC Portal Capabilities and the MetTel response.

Exhibit 2.1.11-3. MetTel TIC Portal Capabilities

TIC Portal Capability	[redacted]
1. TIC Portal Access to External Networks, including the Internet	[redacted]
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 d. Inter-carrier Routing Requirements e. Support to Internet Protocol version 6 (IPv6)	[redacted]
2. EINSTEIN Protection	[redacted]
3. TIC Portal Security Operations Center (SOC)	[redacted]
4. ICD 705 Sensitive Compartmented Information Facility (SCIF)	[redacted]
5. Content Filtering/Inspection of Encrypted Traffic with documented procedures	[redacted]
6. Asymmetric Routing	[redacted]
7. Federal Video Relay Service (FedVRS) Support	[redacted]
8. E-Mail Forgery Protection	[redacted]
9. Signing procedures for outgoing email messages	[redacted]
10. Domain Name System (DNS) and DNS Security Extensions (DNSSEC)	[redacted]

TIC Portal Capability	[redacted]
	[redacted]
11. Uninterrupted Operations	[redacted]
12. Internet Protocol Version 6 (IPv6)	[redacted]
13. Data Loss/Leak Prevention	[redacted]

2.1.11.1.4.2 MTIPS Transport Collection and Distribution Capabilities [L.29.2.1, C.2.8.4.1.4.2]

MetTel team supports the MTIPS Transport Collection and Distribution Capabilities listed below:

1. MetTel allows the agency's Internet bound traffic to reach the Internet via one of the five TIC Portals after passing through either the primary or secondary MTIPS system.
2. MetTel creates a Trusted Domain (DMZ) to ensure that an agency's traffic is protected and physically isolated when transported to the TIC Portal and the public Internet. The DMZ includes the access portion of the service as well as the MTIPS transport. This ensures that the traffic cannot be sniffed nor the ports spoofed.
3. MetTel routes all Inter-agency traffic through the TIC Portal for inspection if the connection is classified as an external connection.

2.1.11.1.5 Features [L.29.2.1, C.2.8.4.2]

Exhibit 2.1.11-4 provides the MetTel team response to the MTIPS features defined in C.2.8.4.2.

Exhibit 2.1.11-4. MetTel MTIPS Architecture Features

Features	[redacted]
1. Encrypted Traffic	[redacted]
2. Agency Security Policy Enforcement	[redacted]

Features	[redacted]
	[redacted]
3. Forensic Analysis	[redacted]
4. Custom Reports	[redacted]
5. Agency NOC/SOC Console	[redacted]
6. Custom Security Assessment and Authorization (A&A) Support	[redacted]
7. External Network Connection	[redacted]
a. Connection shall terminate at an appropriate point	[redacted]
b. In front of the full suite of TIC sensors/capability	[redacted]
c. When over the public networks the VPN shall be encrypted	[redacted]
d. Use of split tunneling	[redacted]
e. Use of Telecommunications Service Priority (TSP)	[redacted]
f. External Network Connection Feature Performance	[redacted]
8. Encrypted DMZ	[redacted]
9. Remote Access	[redacted]
a. VPN connections termination prior to	[redacted]

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

Features	[redacted]
routing through EINSTEIN Enclave	[redacted]
b. VPN terminates in front of MTIPS-managed security controls	[redacted]
c. NIST FIPS 140-2 compliance	[redacted]
d. Telework VPNS disallow split tunneling	[redacted]
e. Multi-factor authentication	[redacted]
f. VPN concentrators and Virtual-Desktop/Application Gateways security	[redacted]
g. Teleworker remote clients use of GFP	[redacted]
h. Teleworker/mobile worker's remote clients use non-GFP	[redacted]
i. Implementation Requirements	
i. TLS and/or IPSec VPNs	[redacted]
ii. VPN Encryption Algorithms	[redacted]
iii. Multi-factor authentication services	[redacted]
iv. Separate DMZ for Remote Access	[redacted]
v. Customized remote access implementations	[redacted]
10. Extranet Connections	[redacted]
a. Connection Termination	[redacted]
b. Terminate in front of the MTIPS-managed security controls	[redacted]

Features	[redacted]
c. VPN Connections over shared public networks	[redacted]
d. Split tunneling shall not be allowed	[redacted]
e. Implementation requirements	[redacted]
f. IPSec VPN from fixed remote locations	[redacted]
g. Multi-Factor Authentication	[redacted]
11. Inventory/Mapping Service	[redacted]

The MetTel system architecture allows for PAs to physically and logically connect to the public Internet or other external connections, as required by the PA, in full compliance with the TIC 2.0 initiative, using MTIPS. Together with the MetTel MPLS network, this forms the PA's TIC Demilitarized Zone (DMZ) for IP traffic. Both the TIC and the MTIPS systems provide capabilities for both IPv4 and IPv6 services.

To meet the External Traffic Routing requirements[redacted] **Exhibit 2.1.11-5** shows the distinct VRF instances on each PE device, allowing the separating of the traffic belonging to different customers. This allows for the logical isolation and independent transport across the common MPLS core of the network.

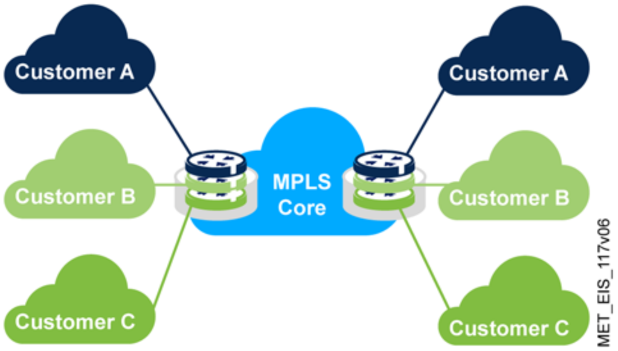

Exhibit 2.1.11-5. MPLS VRF Path Isolation

By default, MetTel will route all of the PA's traffic to the primary MTIPS portal. Each portal is configured with a PA specific configuration for the security services chosen. Internet bound traffic can reach the Internet via the primary MTIPS Portal, with the alternative MTIPS portal configured as a warm back-up, in case the primary MTIPS portal fails. Using standard Border Gateway Protocol (BGP), traffic from the PA's Customer Equipment (CE) router is routed to the primary or secondary MTIPS. In the event the primary MTIPS Portal becomes unavailable for any reason, the BGP session will then announce the PA's routes to a second MTIPS Portal. MetTel will determine the primary and secondary MTIPS Portal for the PA based on capacity, distance, and preference. Load sharing based on IP address can also be accommodated.

[redacted]

Traffic follows the paths detailed above before entering the MTIPS system detailed below in **Exhibit 2.1.11-6**.

[redacted]

Exhibit 2.1.11-6. TIC and MTIPS connections to PA’s

The MetTel team’s MTIPS architecture, illustrated in **Exhibit 2.1.11-6**, is built to meet all of the MTIPS mandatory service requirements as well as provide easy expansion for the optional services. It adheres to all applicable federal and agency-specific IT security directives, standards, policies, and reporting requirements. Future regulation, policies, requirements, standards, and guidelines will have a plan of adoption developed within 90 days of notice.

The MetTel team's MTIPS architecture uses a combination of the security industry's best commercially available technologies to implement the MTIPS requirements. As traffic traverses the MetTel MPLS network and MTIPS system, it is kept logically separate using Virtual Routing and Forwarding (VRF) and Virtual Local Area Network (VLAN) technologies to maintain separation of PAs. Traffic originating from, or destined to the PA's network will be tagged with an agency specific VLAN and encapsulated in a VRF. [redacted]

At the MTIPS border, traffic is identified using the PA's VLAN tags and routed to the appropriate services for that PA. Central to the MTIPS design is an intelligent tap/packet broker that directs traffic to the appropriate services. This broker also provides failsafe operation should failures occur in the DHS GFP or MTIPS systems. IP addresses will be examined to detect and filter spurious/non-agency traffic, which will generate an alert sent to the SOC, as well as to DHS. All of the PA's Internet, Extranet, and inter-agency traffic will be directed to the EINSTEIN enclaves while in transit.

Other services, provided by the MTIPS system are stateless firewalls, DNS firewalling, and mail filtering and sanitization. The firewall can provide URL filtering, and SSL interception and decryption. This enables the encrypted traffic to be analyzed for suspicious patterns that might indicate malicious activity. The firewall will operate in a stateless fashion, providing support for asymmetric traffic routing. The e-mail filtering system will detect domain level sender forgery, as well as other malicious intents. The mail services also offer a level of Data Loss Prevention for the PAs upon request. DNS caching services will provide filtering of DNS queries and validation of DNS Security Extensions for signed domains for MTIPS subscribers. Raw packet capture will also be provided, according to the PA's requirements. The MTIPS architecture fully supports the Federal Video Relay Service for the deaf.

Alerts from a PA's traffic will be consolidated via connector and logger appliances for delivery to the SOC.

Location and system architecture transport SLA KPI performance is measured without the impact of delays within DHS GFP being counted against the system performance. Other KPI's are detailed below.

[redacted]

The SOC will receive data from the two initial MTIPS nodes and reduce, normalize, correlate, fuse and manage the event data from the devices that support the MTIPS operation.

Customized reports will be provided to support the PA's authorities/analysts that will identify security events of interest that may negatively affect the TIC's performance. Properly trained, qualified and cleared staff will support the security functions 24x7. This includes at least 2 people with appropriate credentials to manage the technical aspects of network attacks.

2.1.11.1.6 Interfaces [L.29.2.1, C.2.8.4.3]

MetTel supports the UNIs at the SDP to connect to the MTIPS Transport POP as specified in proposal section 2.1.5.4 [redacted]

2.1.11.1.7 Performance Metrics [L.29.2.1, C.2.8.4.4]

MetTel collects a variety of performance metrics that are monitored by the NOC to ensure the system is always operating within peak efficiency. Reports are available through the MetTel EIS Portal for PA's to access their traffic and equipment performance within the MetTel network.

2.1.11.1.7.1 Performance Metrics for TIC Portal [C.2.8.4.4.1]

Exhibit 2.1.11-7 illustrates the MetTel approach to accomplish, track, and report the performance metrics for the TIC Portal.

Exhibit 2.1.11-7. MetTel Performance Metrics for the TIC Portal

KPI	Type	Performance Standard	Performance Threshold	[redacted]
1. TIC Availability (Av)	Routine	99.5%	≥ 99.5%	[redacted]
	Critical	99.5%	≥ 99.5%	
2. Grade of Service (Failover Time)	Routine	1 minute	≤ 1 minute	[redacted]
3. Grade of Service (Monitoring and Correlation	Routine	Real Time	≤ 4 hours 90% of the time	[redacted]
	Critical	Real Time	≤ 4 hours 99.9% of the time	
4. Grade of Service (Configuration/ Rule Change)	Routine	Within 5 hours for a Normal priority change	≤ 5 hours	[redacted]
		Within 2 hours for a Urgent priority change	≤ 2 hours	
5. EN (Firewall Security Event Notification)	Routine	Within 24 hours of a Low category event	≤ 24 hours	[redacted]
		Within 4 hours of a Medium category event	≤ 4 hours	[redacted]
		Within 30 minutes of a High category event	≤ 30 minutes	[redacted]

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

KPI	Type	Performance Standard	Performance Threshold	[redacted]
				[redacted]
6. EN (Intrusion Detection/ Prevention Security Event Notification)	Routine	Within 24 hours of a Low category event	≤ 24 hours	[redacted]
		Within 10 minutes of a High category event	≤ 10 minutes	[redacted]
7. Grade of Service (Virus Protection Updates and Bug Fixes)	Routine	Normal Priority Update 24 hours	≤ 24 hours	[redacted]
		Urgent Priority Update 2 hours	≤ 2 hours	[redacted]

2.1.11.1.7.2 Performance Metrics for MTIPS Transport Collection and Distribution [C.2.8.4.4.2]

Our imbedded performance collection and management capabilities provide real-time and historic reporting of the Acceptable Quality Levels (AQL) of the performance metrics for the MTIPS Transport Collection and Distribution. [redacted] via the Management and Maintenance element of the MetTel EIS Portal, and the Trouble Ticketing element of the MetTel Portal maintains and reports time-to-restore. The MetTel SOC provides security incident reporting via ATIP. Exhibit 2.1.12-8 illustrates the MetTel approach to accomplish, track, and report the performance metrics for the MTIPS transport collection and distribution.

Exhibit 2.1.11-8. MetTel Performance Metrics for MTIPS Transport Collection and Distribution

KPI	Type	Performance Threshold	AQL	[redacted]
Availability of Port	Routine	99.95%	≥ 99.95%	[redacted]
	Critical	99.995%	≥ 99.995%	
Latency (CONUS)	Routine	60 ms	≤ 60 ms	[redacted]
	Critical	50 ms	≤ 50 ms	
GOS (Data Delivery Rate)	Routine	99.95%	≥ 99.95%	[redacted]
	Critical	99.995%	≥ 99.995%	
Time to Restore	Without dispatch	4 hours	≤ 4 hours	[redacted]
	With dispatch	8 hours	≤ 8 hours	
EN (Security Incident Report)	Routine	Near real time	≤ 30 min	[redacted]