ENTERPRISE INFRASTRUCTURE SOLUTIONS (EIS) ACQUISITION

Contract No. GS00Q17NSD3007

May 14, 2019

Submitted by:

MetTel

55 Water Street, 32nd Fl.

New York, NY 10041

Submitted to:

General Services Administration

Office of Integrated

Technology Services

1800 F St., NW

Washington, DC 20405

Volume 1 Technical Volume

TABLE OF CONTENTS

ENTERPRISE INFRASTRUCTURE SOLUTIONS (EIS) ACQUISITION 1
LIST OF EXHIBITS III
LIST OF ACRONYMS X
1 NETWORK ARCHITECTURE [L.29.1, M.2.1, C.1.1, C.1.6, C.1.8.6] 1
1.1 Understanding [L.29.1(A), M.2.1(1), C.1.8.4] 2
1.1.1 MetTel EIS Portal 14
1.2 Quality of Services [L.29.1 (B), M.2.1 (2), C.1.8.2, C.1.8.3] 22
1.3 Service Coverage (for CBSA-dependent services) [L.29.1(C), M.2.1 (3), C.1.3, C.1.8.5] 23
1.4 Security L.29.1(D), M.2.1(4)] 24
2. TECHNICAL RESPONSE [L.28.2] 27
2.1 EIS Services [L.29.2.1, M.2.1, C.1.2, H.16; H.17; H.18; H.20; H.24] 28
2.1.1 Virtual Private Network Service [C.2.1.1] 31
2.1.2 Ethernet Transport Service [C.2.1.2] 43
2.1.3 Internet Protocol Voice Service [C.2.2.1] 52
2.1.4 Managed Network Services [C.2.8.1] 74
2.1.5 Access Arrangements [C.2.9, F.2.1 (28)] 90
2.1.6 Internet Protocol Service [C.2.1.7] 102
2.1.7 Circuit Switched Voice Service [C.2.2.2] 108
2.1.8 Colocated Hosting Service [C.2.4] 117
2.1.9 Wireless Service [C.2.6] 122
2.1.10 Unified Communications Service [C.2.8.3] 129
2.1.11 Managed Trusted Internet Protocol Service [C.2.8.4] 146
2.1.12 Managed Security Service [C.2.8.5] 164
2.1.13 Managed Mobility Service [C.2.8.6] 181
2.1.14 DHS Intrusion Prevention Security Service [C.2.8.9] 199
2.1.15 Service Related Equipment [C.2.10, Section D] 219
2.1.16 Service Related Labor [C.2.11, B.2.11.2; J.5; J.9; J.10] 224
2.1.17 Cable and Wiring [C.2.12, J.9] 226

2.1.18 Toll Free Service [C.2.2.3] 227
2.1.19 Circuit Switched Data Service (CSDS) [C.2.2.4] 241
2.1.20 Audio Conferencing Service [C.2.8.7] 245
2.1.21 Private Line Service (PLS) [C.2.1.4] 252
2.2 Information Security [L.11, L.29.2.2, J.14] 259
2.3 External Traffic Routing Requirement [L.29.2.3, C.1.8.8] 260
2.3.1 Methodology for Identifying Agency Traffic [L.29.2.3 (1)] 261
2.3.2 Approach to Redirecting Agency Traffic to EINSTEIN [L.29.2.3 (2)] 264
2.3.3 Approach to Notify DHS of Non-Participating Agency Traffic [L.29.2.3 (3)] 277
2.3.4 Control Mechanisms to Ensure No By-Pass [L.29.2.3 (4)] 278
2.3.5 Sensing and Control Mechanisms to Ensure Traffic Failsafe [L.29.2.3 (5)] 278
2.3.6 Location of Certified Facilities [L.29.2.3 (6)] 279
2.3.7 Availability of TS/SCI-Cleared Personnel [L.29.2.3 (7)] 279
2.3.8 Instrumentation to Measure Transport KPIs [L.29.2.3 (8)] 280
3.0 SATISFACTION OF 508 REQUIREMENTS [C.4, F.2.1(33)] 281

LIST OF EXHIBITS

Exhibit 1-1. Features and Benefits of MetTel Network Architecture 1
Exhibit 1-2. MetTel Network Architecture Support by Service 3
Exhibit 1-3. Telecommunications Synergy 4
Exhibit 1-4. MetTel Network Architecture 6
Exhibit 1-5. MetTel POP Architecture 8
Exhibit 1-6. Customer Dedicated Connection Architecture 10
Exhibit 1-7. MetTel Network Access Architecture 11
Exhibit 1-8. Embedded Services Architecture 12
Exhibit 1-9. MetTel EIS Service Management Architecture 13
Exhibit 1-10. MetTel EIS Portal Ordering Functions 14
Exhibit 1-11. MetTel EIS Portal Inventory Management 15

Exhibit 1-12. Trouble Ticket Management 16
Exhibit 1-13. Network Monitoring and Management 17
Exhibit 1-14. MetTel EIS Portal Billing Summary 18
[redacted]
Exhibit 1-17. Example CoS Implementation 22
[redacted]
Exhibit 1-19. MetTel Global Network Reach 24
Exhibit 2.1-1. MetTel EIS Proposed Services 28
Exhibit 2.1.1-1. Features and Benefits of Approach to VPNS 31
Exhibit 2.1.1-2. MetTel MPLS Core VPNS Backbone 33
[redacted]
Exhibit 2.1.1-5. Link and Traffic Monitoring 35
Exhibit 2.1.1-6. Standards Utilization 36
Exhibit 2.1.1-7. Security Technical Capabilities Support 37
Exhibit 2.1.1-8. Connectivity and Quality of Service Technical Capabilities Support 38
Exhibit 2.1.1-9. Load Sharing Configurations for VPNS 39
Exhibit 2.1.1-10. Failover Configurations for VPNS 40
Exhibit 2.1.1-11. Diverse Access Points to MetTel POPs for VPNS 41
Exhibit 2.1.2-1. Features and Benefits of MetTel's Approach to ETS 43
Exhibit 2.1.2-2. Ethernet Service Architecture 45
Exhibit 2.1.2-3. E-Line Extended Delivery Model 46
Exhibit 2.1.2-4. E-LAN Extended Delivery Model 47
Exhibit 2.1.2-5. MetTel Ethernet Partner Service Providers 48
Exhibit 2.1.2-6. Ethernet Transport Service Technical Capabilities 48
Exhibit 2.1.3-1. Features and Benefits of MetTel's Approach to IPVS 53
[redacted]
Exhibit 2.1.3-3. MetTel Converged IPVS 56
Exhibit 2.1.3-4. Global Reach for IP Voice Services 56
Exhibit 2.1.3-5. MetTel Voice Architecture 58

Exhibit 2.1.3-6. MetTel IPVS Technical Capabilities 58
[redacted]
Exhibit 2.1.3-8. IPVS User and Administrator Capabilities 63
Exhibit 2.1.3-9. MOS and RTT Performance Display 67
Exhibit 2.1.3-10. MetTel SIP Trunk Solutions 71
Exhibit 2.1.3-11. MetTel SIP Trunk Architecture 73
Exhibit 2.1.4-1. Features and Benefits of the MetTel Solution 74
[redacted]
Exhibit 2.1.4-3. MetTel MNS Comprehensive Solutions 79
Exhibit 2.1.4-4. Customer Care 80
Exhibit 2.1.4-5. Sample Configuration Change Process 81
Exhibit 2.1.4-6. Customer Care Services for MNS Agencies 82
[redacted]
Exhibit 2.1.4-8. MetTel EIS Portal Network Performance Examples 85
Exhibit 2.1.4-9. MetTel EIS Portal Network Performance Information 85
Exhibit 2.1.4-10. MetTel Portal Equipment Inventory Information 86
Exhibit 2.1.4-11. MetTel Trouble Ticket Management 87
Exhibit 2.1.5-1. Features and Benefits of MetTel Access Arrangements 90
Exhibit 2.1.5-2. Diverse Paths from the SDP to Two Diverse Contractors' POPs 92
Exhibit 2.1.5-3. Diverse Paths from the SDP to Two Providers' POPs 92
Exhibit 2.1.5-4. Physically Diverse Paths to a Single MetTel POP 93
Exhibit 2.1.5-5. Redundant Paths from an SDP to the MetTel POP 94
Exhibit 2.1.5-6. Redundant and Disparate Paths from an SDP to the MetTel POP 94
Exhibit 2.1.5-7. Supported Access Arrangements and Standards 96
Exhibit 2.1.5-8. SRE Interfaces for AA UNIs 100
Exhibit 2.1.6-1. Features and Benefits of Approach to IPS 102
Exhibit 2.1.6-2. Preferred Partner Reach for IPS 104
Exhibit 2.1.6-3. MetTel IPS Capabilities 105
Exhibit 2.1.6-4. IPS QoS Traffic Priority Classes 106
Exhibit 2.1.6-5. IPS Supported Interface Types (UNI) 107
Exhibit 2.1.7-1. Features and Benefits of Approach to CSVS 108

Exhibit 2.1.7-2. CSVS and IPVS Integration 110
Exhibit 2.1.7-3. CSVS Supported Terminations 111
Exhibit 2.1.7-4. CSVS Technical Capabilities 111
Exhibit 2.1.7-5. CSVS Features 112
Exhibit 2.1.9-1. Features and Benefits of Approach to MWS 122
Exhibit 2.1.9-2. MetTel MWS Device Capabilities 125
Exhibit 2.1.9-3. MetTel MWS Service Plans 126
Exhibit 2.1.9-4. MetTel MWS Features 127
Exhibit 2.1.10-1. Features and Benefits of Approach to UCS 130
[redacted]
Exhibit 2.1.10-3. Standards Response and Discussion. 134
Exhibit 2.1.10-4. Unified Messaging (UM) Capabilities 136
Exhibit 2.1.10-5. Mobile Integration Capabilities. 137
Exhibit 2.1.10-6. Unified User Interface. 137
[redacted]
[redacted]
Exhibit 2.1.11-1 MTIPS Configuration and High Level Data Flow 147
Exhibit 2.1.11-2. Features and Benefits of MetTel MTIPS Architecture 148
Exhibit 2.1.11-3. MetTel TIC Portal Capabilities 152
Exhibit 2.1.11-4. MetTel MTIPS Architecture Features 153
Exhibit 2.1.11-5. MPLS VRF Path Isolation 157
Exhibit 2.1.11-6. TIC and MTIPS connections to PA's 158
Exhibit 2.1.11-7. MetTel Performance Metrics for the TIC Portal 161
Exhibit 2.1.11-8. MetTel Performance Metrics for MTIPS Transport Collection and Distribution 163
Exhibit 2.1.12-1. Features and Benefits of the Raytheon Solution 164
Exhibit 2.1.12-2. Raytheon's MSS 166
Exhibit 2.1.12-3. Raytheon's [redacted] Client Interface 167
[redacted]
Exhibit 2.1.12-5. Raytheon's MSS Flow 170
Exhibit 2.1.12-6. Raytheon's Four Phase Vulnerability Testing Methodology 171

Exhibit 2.1.12-7. Scoping 172
Exhibit 2.1.12-8. Profiling Target Environment 172
Exhibit 2.1.12-9. Commonly Used Tools 173
Exhibit 2.1.12-10. Testing Phase 173
Exhibit 2.1.12-11. Reporting Phase 174
Exhibit 2.1.12-12. Raytheon INRS Capabilities 176
Exhibit 2.1.12-13. Raytheon INRS Handling Methodology 178
Exhibit 2.1.12-14. Raytheon MPS Features 178
Exhibit 2.1.13-1. Features and Benefits of Approach to MMS 182
Exhibit 2.1.13-2. MDM Capabilities of MMS [redacted] 184
Exhibit 2.1.13-3. MDM Device Enrollment Capabilities 186
Exhibit 2.1.13-4. MMS Device Profiles 187
Exhibit 2.1.13-5. MMS Device Feature Management Capabilities 188
Exhibit 2.1.13-6. Additional MDM Capabilities 189
Exhibit 2.1.13-7. Application Deployment 190
Exhibit 2.1.13-8. Mobile Application Store 191
Exhibit 2.1.13-9. MAM Application Security 191
Exhibit 2.1.13-10. MAM Optional Capabilities 192
Exhibit 2.1.13-11. Mobile Security Capabilities of MMS 193
Exhibit 2.1.13-12. Mobile Deployment Support 196
Exhibit 2.1.14-1. Features and Benefits of Approach to IPSS 200
[redacted]
Exhibit 2.1.14-5. Required Technical Capabilities 214
Exhibit 2.1.15-1. Features and Benefits of Approach to SRE. 219
Exhibit 2.1.16-1. Features and Benefits of Approach to SRL. 224
Exhibit 2.1.17-1. Features and Benefits of Approach to CW. 226
Exhibit 2.1.18-1. Features and Benefits of Approach to TFS 227
Exhibit 2.1.18-2: MetTel's Support of Required Standards 228
Exhibit 2.1.18-3: MetTel's TFS Meets All EIS Section C.2.2.3.1.4 Requirements 229

Exhibit 2.1.18-4: MetTel's TFS Meets all Feature Requirements of EIS Section C.2.2.3.2 230
Exhibit 2.1.18-5. MetTel's Support for TFS Reporting Features 236
Exhibit 2.1.18-6. Interfaces supported by MetTel's TFS 239
Exhibit 2.1.18-7. MetTel's TFS Meets the Complete Set of Performance Requirements of EIS Section C.2.2.3.4 240
Exhibit 2.1.19-1. Features and Benefits of Approach to TFS 241
Exhibit 2.1.20-1. Features and Benefits of Approach to TFS 245
[redacted]
Exhibit 2.1.20-3: MetTel's Audio Conferencing Service Technical Capability 247
Exhibit 2.1.20-4: Features of MetTel's ACS Solution 249
Exhibit 2.1.20-5: Performance Metrics for MetTel's ACS Solution 250
Exhibit 2.1.21-1. MetTel's Complies with all PLS Evaluation Criteria and Requirements 252
Exhibit 2.1.21-2. MetTel's PLS Adheres to the Full Range of Industry Standards 254
Exhibit 2.1.21-3. General Technical Capabilities of MetTel's PLS 255
Exhibit 2.1.21-4. MetTel's PLS Supports the Full Range of Data Rate Categories 255
Exhibit 2.1.21-5. MetTel's PLS Meets All Feature Requirements 256
Exhibit 2.1.21-6. MetTel's PLS Supports a Wide Range of Interface Options for Agencies 257
Exhibit 2.1.21-7. Performance Metrics for MetTel's PLS Solution 258
Exhibit 2.3-1. MPLS Device Roles 262
[redacted]

[redacted]

Exhibit 3-1. Section 508 Requirements for MetTel EIS Services..... 281

LIST OF ACRONYMS

Acronym	Definition
A&A	Assessment and Authorization
AA	Access Arrangements
ACD	Automatic Call Distribution
ACE	App Configuration for Enterprise
AD	Active Directory
AES	Advanced Encryption Standard
AF2	Assured Forwarding Class 2
AF3	Assured Forwarding Class 3
AF31	Assured Forwarding Class 3 with Low Drop Precedence
AF4	Assured Forwarding Class 4
AGS	AirWatch Government Services
ALG	Application Layer Gateways
ALI	Automatic Location Identification
ANI	Automatic number identification
ANSI	American National Standards Institute
ANSI/TIA-942	Telecommunications Infrastructure Standard for Data Centers
AOL	America Online
API	Application Program Interface
APT	Advanced Persistent Threat
AQL	Acceptable Quality Levels
ARIN	American Registry of Internet Numbers
AS16524	Autonomous System Number for MetTel Network
ASA	Adaptive Security Appliance - Cisco
ASR	Aggregation Service Router - Cisco
AT	Awareness and Training - NIST SP 800-53 rev 4

Acronym	Definition
ATIP	Automated Threat Intelligence Platform
ATIS	Alliance for Telecommunications Industry Solutions
ATO	Authority to Operate
B/BX/PX	Ethernet Interface Definitions
BE	Best Effort
BGP	Border Gateway Protocol
BGP/MPLS	BGP used in conjunction with an MPLS network
BI	Business Intelligence
BRI	Basic Rate Interface
BYOD	Bring Your Own Device
CA	Security Assessment and Authorization - NIST SP 800-53 rev 4
CAC	Common Access Card
CAC/PIV	Common Access Card (CAC), with Personal Identity Verification (PIV)
CALEA	Communications Assistance of Law Enforcement Act
CAP	Compliance and Assurance Program
CBS	Committed Burst Size
CBSA	Core Based Statistical Area
CCM	Counter with CBC-MAC is a mode of operation for cryptographic block ciphers
CCV	Compliance Validation
CDMA	Code Division Multiple Access
CDR	Call Data Record
CDS	Cross Domain Solution
CE	Customer Edge
CERT	Computer Emergency Readiness Team

Acronym	Definition
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CLEC	Competitive Local Exchange Carrier
CNMI	Commonwealth of Northern Marianas Islands
CNNSP-15	Committee on National Security Systems. Policy No. 15.
CODEC	Encoder-Decoder
CONUS	Continental United States
CoS	Class of Service
CoSR	Class of Service Restriction
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CRM	Customer Relationship Management
CS	Certificate Services
CS&C	Cybersecurity and Communications
CS-4000	Multi-function platform for controlling and securing next generation services
CSA	Cloud Security Alliance
CSO	Customer Support Office
CSU/DSU	Channel Service Unit/Data Service Unit
CSVS	Circuit Switched Voice Service
CTIA	Cellular Telecommunications and Internet Association
CUI	Controlled Unclassified Information
CW	Cable and Wiring
DC3500	Sourcefire Defense Center 3500
DDoS	Distributed Denial of Service
DFIR	Digital Forensics and Incident Response
DHS	Department of Homeland Security

Acronym	Definition
DID	Direct Inward Dialing
DISA	Defense Information Systems Agency
DLP	Data Loss Protection
DMVPN	Cisco Dynamic Multipoint VPN
DMZ	Demilitarized Zone
DNS	Domain Name Service
DNSSEC	DNS Security Extensions
DOCSIS	Data Over Cable Service Interface Specification
DoD	Department of Defense
DoS	Denial of Service
DR	Disaster Recovery
DS	Differentiated Services
DS0	Digitial Signal 0 is basic signaling rate of 64 kbps
DS1	Digital Signal 1 is full duplex circuit at 1.544 Mbits
DS3	Digital Signal 3 is full duplex circuit at 44.736 Mbits
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DWDM	Dense wavelength division multiplexing
E-LAN	Ethernet Private Local Area Network
E-LINE	Ethernet Private Line
E3A	Einstein 3 Accelerated
EAD	Enterprise Active Directory
ECS	Enhanced Cybersecurity System
EDI	Electronic Data Interchange
EF	Expedited Forwarding

Acronym	Definition
EIA	Electronic Industries Association
EIGRP	Enhanced Interior Gateway Routing Protocol
EINSTIEN	The Department of Homeland Security (DHS) has the mission to provide a common baseline of security across the federal civilian executive branch and to help agencies manage their cyber risk. This common baseline is provided in part through the EINSTEIN system
EIS	Enterprise Infrastructure Solutions
EMEA	Europe, Middle East, Africa
EMM	Enterprise Mobility Management
EnCE	EnCE® certification acknowledges that professionals have mastered computer investigation methodology as well as the use of EnCase® software during complex computer examinations.
ENNI	External Network Network Interface – MEF 26.1
ePO	McAfee ePolicy Orchestrator (McAfee ePO) is the most advanced, extensible, and scalable centralized security management software in the industry.
ESA	Email Security Appliance
ESF	Extended superframe
ESM	McAfee Enterspise Security Manager
ESP	Encapsulating Security Payload
ETS	Ethernet Transport Service
ETS-15	Ethernet Transport Service UNI-15
ETSI	European Telecommunications Standards Institute
EVC	Ethernet Virtual Connections
EVDO	Evolution-Data Optimized is a telecommunications standard for the wireless transmission of data through

Acronym	Definition
	radio signals, typically for broadband Internet access.
FCC	Federal Communications Commission
CRTC	Canadian Radio-Television and Telecommunications Commission
FIFO	First in, First out
FIPS	Federal Information Processing Standard
FISMA	
FMC	Fixed Mobile Convergence
FOC	Firm Order Commitment
FS-ISAC	Financial Services-Information Sharing and Analysis Center
FTK	Forensic Toolkit
FTTP	Fiber to the Premise
FX	Fiber encoded hand off for Ethernet
GB	Gigabyte
GCFA	GIAC Certified Forensic Analyst
GCIA	GIAC Certified Intrusion Analyst
GCIH	GIAC Certified Incident Handler
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFP	Government Furnished Property
GIAC	Global Information Assurance Certification
GLBP	Gateway Load Balancing Protocol
GOS	Grade of Service
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GREM	GIAC Reverse Engineer Malware

Acronym	Definition
GSA	General Services Administration
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability Act
HSPDA	High-Speed Downlink Packet Access
HSRP	Hot Standby Router Protocol
HTTP/HTTPS	Hypertext Transfer Protocol/ Hypertext Transfer Protocol Secure
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation, and Air Conditioning
I&A	Intelligence and Analysis
IAD	Integrated Access Device
ICD	Intelligence Community Directive
ICE	Interactive Connectivity Establishment
ICE/STUN/TURN	Interactive Connectivity Establishment/Session Traversal Utilities for NAT/ Traversal Using Relays around NAT
ICMP	Internet Control Message Protocol
ID	Identification
IDS	Intrusion Detection System
IDS/IPS	Intrusion Detection System/Intrusion Protection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IETF-TLS	Internet Engineering Task Force - Transport Layer Security
ILEC	Incumbent Local Exchange Carrier
IM&P	Instant Messaging Presence
IMAP	Internet Message Access Protocol

Acronym	Definition
IMAP4	Internet Mail Access Protocol V4
IMS	IP Multimedia Subsystem
INR	Incident Response
INRS	Incident Response Services
IOC	Indicators of Compromise
iOS	Apple mobile device operating system
IoT	Internet of Things
IP	Internet Protocol
IP/PPP	Internet Protocol/Point-to-Point
IPDS	Intrusion Prevention and Detection Systems
IPS	Internet Protocol Service
IPsec	IP Security
IPSLA	Cisco Internet Protocol Service Level Agreement Package
IPSS	Intrusion Prevention Security Service
IPVS	Internet Protocol Voice Service
IRS	Internal Revenue Service
ISDN	Integrated Services for Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISV	Independent Software Vendors
IT	Infromation Technology
ITT	Information Technology Tools
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
ITU-TSS	International Telecommunications Union-Telecommunications Service Sector
IVR	Interactive voice response

Acronym	Definition
J-STD-025	This Standard defines the interfaces between a telecommunication service provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance.
JAB	Joint Authorization Board
KHz	Kilohertz is a unit of frequency
KPI	Key Performance Indicator
KTS	Key Telephone Systems
L2TP	Layer 2 Tunneling Protocol
L2TP/IPSec	Layer 2 Tunneling Protocol over IPSec
L3VPN	Layer 3 Virtual Private Network
LAES	Lawfully Authorized Electronic Surveillance
LAN	Local Area Network
LAN-LAN	LAN to LAN Connection
LD	Long Distance
LDAP	Lightweight Directory Access Protocol
LEC	Local Exchange Carriers
LLDP	Link Layer Discovery Protocol
LSP	Label Switched Paths
LTE	Long Term Evolution
LX	Ethernet interface for long wavelength for a "long haul" fiber optic cable for a maximum length of 10 kilometers
M2M	Machine to Machine
MACD	Moves Adds Changes Disconnects
MACSec	Media Access Control Security
MADP	Mobile Application Development Platforms
MAE-East	Metropolitan Area Exchange-East

Acronym	Definition
MAE-West	Metropolitan Area Exchange-West
MAM	Mobile Application Management
MAS	Mobile Applications Store
MBS	Maximum Burst Size
MCM	Mobile Content Management
MD5	Message-digest algorithm used cryptographic hash function producing a 128-bit (16-byte) hash value.
MDM	Mobile Device Management
MEF	Metro Ethernet Forum
MGCP	Media Gateway Control Protocol
MIB	Management Information Bases
MTIPS	Managed Trusted Internet Protocol Services
MKA	MACSec Key Agreement
MLPP	Multilevel Precedence and Preemption
MLPPP	Multi Link Point to Point Protocol
MMS	Managed Mobility Service
MNS	Managed Network Service
MOE	Mission Operating Environment
MOE-C	Mission Operating Environment-Classified
MOS	Mean Opinion Score
MPKI	Managed Public Key Infrastructure
MPLS	Multi Protocol Label Switching
MPLS-TP	Multi Protocol Label Switching-Transport Profile
MPS	Managed Prevention Services
MSEC	Multi Service Ethernet Connections
MSS	Managed Security Service
MTIPS	Managed Trusted Internet Protocol Service

Acronym	Definition
MTLS	Multiplexed Transport Layer Security
MUX	Multiplexer
MWS	Mobile Wireless Service
MX	Mail Exchanger
N/A	Not Applicable
NAC	Network Access Control
NAT	Network Address Translation
NCCIC	National Cybersecurity and Communications Integration Center
NCS	New Client Services
NCSD	National Cyber Security Division
NFC	Near Field Communications
NFV	Network Function Virtualization
NFV/SDN	Network Function Virtualization/Software Defined Network
NIST	National Institute of Standards and Technology
NNI	Network Network Interfaces
NOC	Network Operations Center
NOC/SOC	Network Operations Center/ Security Operations Center
NPA	Numbering Plan Area
NS/EP	National Security and Emergency Preparedness
NS2020	NETWORK SERVICES 2020
NSM	Network Security Monitor
NXX	Numbering Plan Exchange
O&M	Operations and Maintenance
OCO	Ordering Contracting Officer
OCONUS	Outside Contiguous United States
OCx	Optical Carrier Levels

Acronym	Definition
OEM	Original Equipment Manufacturers
OMB	Office of Management and Budget's
OS	Operating System
OTA	Over the Air
PA	Participating Agencies
PAT	Port Address Translation
PBX	Private Branch Exchange
PC	Personal Computer
PC/RT	Windows Operating System for Mobile Devices
PCAP	Packet Capture
PCI DSS	Payment Card Industry Data Security Standard
PCL	Physical Concentration Locations
PCM	Pulse Code Modulation
PDA	Personal Digital Assistant
PDF	Portable Document Format
PE	Provider Edge
PE-PE	Provider Edge to Provider Edge
PIDF	Presence Information Data Format
PII	Personally Identifiable Information
PIM	Personal Information Management
PIR	Peak Information Rate
PIV	Personal Identity Verification
PIV/CAC	Personal Identity Verification/ Common Access Card
PKI	Public Key Encryption
PLS	Private Line Service
PM	Performance Monitoring

Acronym	Definition
PMO	Program Management Office
POA&M	Plan of Action and Milestones
PoC	Points of Contact
POP	Points of Presence
POP3	Post Office Protocol 3
PPP	Point to Point Protocol
PPTP	Point to Point Tunneling Protocol
PRI	Primary Rate Interface
PS/ALI	Private Switch/Automatic Location Identification
PSAP	Public Safety Answering Point
PSK	Pre-shared Key
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuits
QoS	Quality of Service
RACI	Responsible Accountable Consult or Inform
RAD	Rapid App Development
RC4	Encryption Algorithm, developed by RSA, is a shared key stream cipher algorithm requiring a secure exchange of a shared key.
RFC	Request for Comments
RFP	Request for Proposal
RSA	Rivest-Shamir-Adleman founders now RSA Security
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource ReSerVation Protocol
RT	Response Time
RTP	Real-Time Transport Protocol
RTT	Round Trip Delay Time

Acronym	Definition
S&CSI	Security and Common Services Infrastructure
SAN	Storage Area Networks
SBC	Session Border Controllers
SCAP	Security Content Automation Protocol
SCCP	Skinny Client Control Protocol
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCRM	Supply Chain Risk Management
SD	Software Defined
SD-WAN	Software Defined Wide Area Network
SDK	Software Development Kit
SDN	Software Defined Network
SDP	Service Delivery Point
SDSL	Symmetric DSL
SECONOP	Security Concept of Operations
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SIP/SDP	Session Initiation Protocol (SIP) and Session Description Protocol (SDP)
SLA	Service Level Agreement
SME	Subject Matter Experts
SMS	Short Messaging Services
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SONET	Synchronous Optical Network
SOO	Statement of Objectives

Acronym	Definition
SOP	Standard Operating Procedures
SP	Special Publication
SQL	Structured Query Language
SRE	Service Related Equipment
SRL	Service Related Labor
SRTM	Security Requirements Traceability Matrix
SRTP	Secure Real-Time Transport Protocol
SSL	Secure Sockets Layer
SSL/TLS	Secure Sockets Layer and Transport Layer Security
SSLVPN	Secure Sockets Layer Virtual Private Network
SSP	System Security Plan
STIG	Security Technical Implementation Guide
SVE	Service Verification Environment
SWC	Serving Wire Centers
T/TX/FX	Ethernet 100 Base Interfaces
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexing
TEM	Telecommunications Expense Management
TIC	Trusted Internet Connection
TIC/MTIPS	Trusted Internet Connection/ Managed Trusted Internet Protocol Service
TICAP	Trusted Internet Connection Access Provider
TLS	Transport Layer Security
TMS	Trouble Management System
ToS	Type of Service

Acronym	Definition
TS	Top Secret
TS/SCI	Top Secret/Sensitive Compartmented Informaition
TSP	Telecommunications Service Priority
TSS	Telecommunication Standardization Sector
SR-TSV-002275	Telcordia standard for two wire analog lines
TT	Trouble Ticket
TTM	Trouble Ticket Management
TTR	Time to Restore
TTY	Text Telephone
U.S.	United States
U.S.	Ubiquitous Service
UC	Unified Communications
UCS	Unified Communication Service
UM	Unified Messaging
UNI	User-to-Network Interface
URL	Universal Resource Locator
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
USC	United States Code
USCERT	United States Computer Emergency Readiness Team
USDA	United Stated Department of Agriculture
V&V	Verification and validation
VA	Virginia
VDI	Virtual Desktop Infrastructure
VDI/ALG	Virtual Desktop(VDI)/Application Layer Gateways (ALG)
VLAN	Virtual LAN

Acronym	Definition
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VPNS	Virtual Private Network Service
VRF	Virtual Routing and Forwarding
VRF/BGP	Virtual Routing and Forwarding/ Border Gateway Protocol
VRRP	Virtual Router Redundancy Protocol
VSAT	Very Small Aperture Terminal
VSS	Vulnerability Scanning Services
VTI	Virtual Tunnel Interface
WAV	WAVe form audio format
WCCP	Web Cache Communication Protocol
WCDMA	Wideband Code Division Multiple Access
WCS	Web Conferencing Service
WDM	Wavelength Division Multiplexing
WMA	Washington Metropolitan Area
WPS	Wireless Priority Service
xDSL	Refers collectively to all types of digital subscriber lines
XMPP	Extensible Messaging and Presence Protocol
XMPP/SIP/PIDF	Extensible Messaging and Presence Protocol (XMPP)/ Session Initiation Protocol (SIP)/ Presence Information Data Format (PIDF)

1 NETWORK ARCHITECTURE [L.29.1, M.2.1, C.1.1, C.1.6, C.1.8.6]

The MetTel network architecture meets the mandatory service requirements in SOW paragraph C.1.2. This section presents a technical description of our offering, demonstrating our extensive capabilities in Standards, Connectivity, Technical Capabilities, Features, Interfaces, Performance Metrics, and Security. **Exhibit 1-1** highlights some key strengths and benefits of our EIS solution in relation to RFP section M.2.1 evaluation criteria.

MetTel Strengths
Small Business, Large Reach

- True facilities-based telecom integrator
- Global reach
- [redacted]
- MetTel EIS Portal—one stop information source including Inventory, Billing, MACD, Procurement, and more
- Award winning customer support

Exhibit 1-1. Features and Benefits of MetTel Network Architecture

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• Network architecture meets all requirements for IPVS, ETS, MNS, VPNS and AA. [redacted] • Architecture supports all 17 proposed services • 20 years of experience as a true facilities-based telecommunications integrator [redacted] • MetTel's [redacted] is built with the latest-technology hardware and software configured to be extremely flexible and reliable
Quality of Services (M.2.1(2))	[redacted] Network that provides reliable and [redacted] • 24x7 live customer support through multiple NOCs and [redacted]
Service Coverage (M.2.1(3))	[redacted] Network architecture that provides scalable, expansive reach with comprehensive connection options through [redacted]
Security (M.2.1(4))	• [redacted]

Evaluation Criteria	Features and Benefits of MetTel's Approach
	[redacted] • MetTel complies with the security requirements of the Mandatory Service and the designated optional service definitions. • MetTel 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. • [redacted] • MetTel supports the proper safeguards for handling traffic should failures occur with the [redacted]

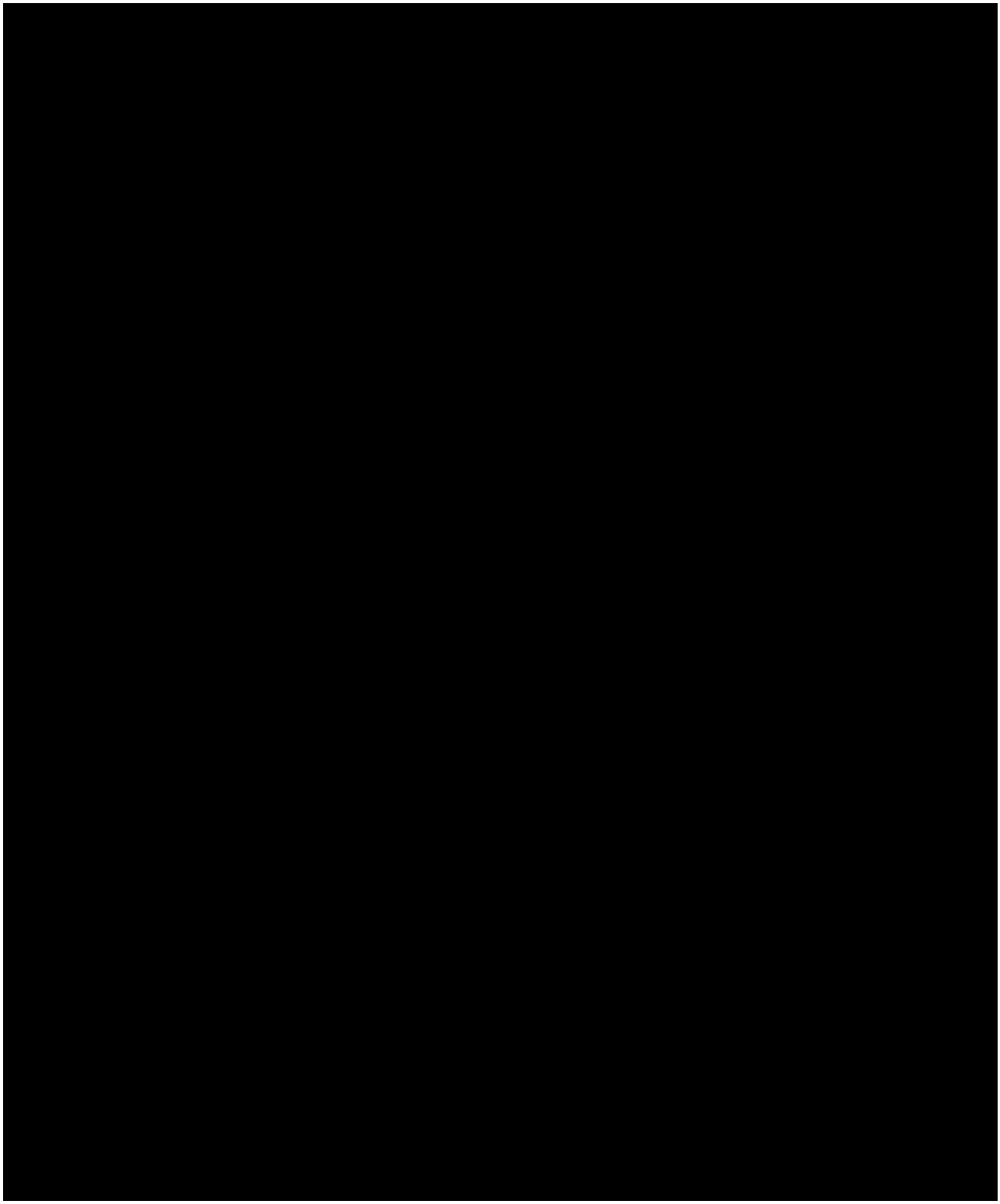
1.1 Understanding [L.29.1(A), M.2.1(1), C.1.8.4]

MetTel Network
The Most Comprehensive Reach in the Industry

- Single source, converged, secured networks [redacted]
- Largest Nationwide Footprint
- Dedicated Government Care Team

MetTel provides the Government access to one of the most robust networks available. Even as a [redacted] **Exhibit 1-2** shows how the MetTel network architecture supports the proposed EIS services. The MetTel EIS Portal supports all EIS services, providing Agencies with a single view of all service information. MetTel will make available any future service interoperability [redacted] when MetTel offers the interoperability for its commercially provided service.

Exhibit 1-2. MetTel Network Architecture Support by Service



Connectivity and Service Areas

Since inception, the MetTel service philosophy has been to act as a value added

strategic partner and single source for all of our customers' telecommunications requirements. As a combined telecommunications integrator and network services provider, we [redacted]

As an end-to-end Communications Solutions Provider we bring true harmony to the telecommunication service life cycle. Considering the ever-evolving landscape of this

[redacted]

Exhibit 1-3. Telecommunications Synergy

industry, where very large companies are being bought and sold at alarming rates and networks are attacked at unprecedented rates, [redacted]

Several of MetTel's partners are exceptional leaders in their field and as such provide key elements of the MetTel service offering.

[redacted]

Our scale and relationships provide MetTel Government customers with the lowest cost and best coverage across multiple products and solutions, combining the best-of-the-best. MetTel enables Government mission-critical objectives and increases efficiencies to end users. MetTel works closely with all of our partners and providers to design, develop, and install solutions all supported by our award winning customer service. **Exhibit 1-4** provides a high level overview of the MetTel network architecture.

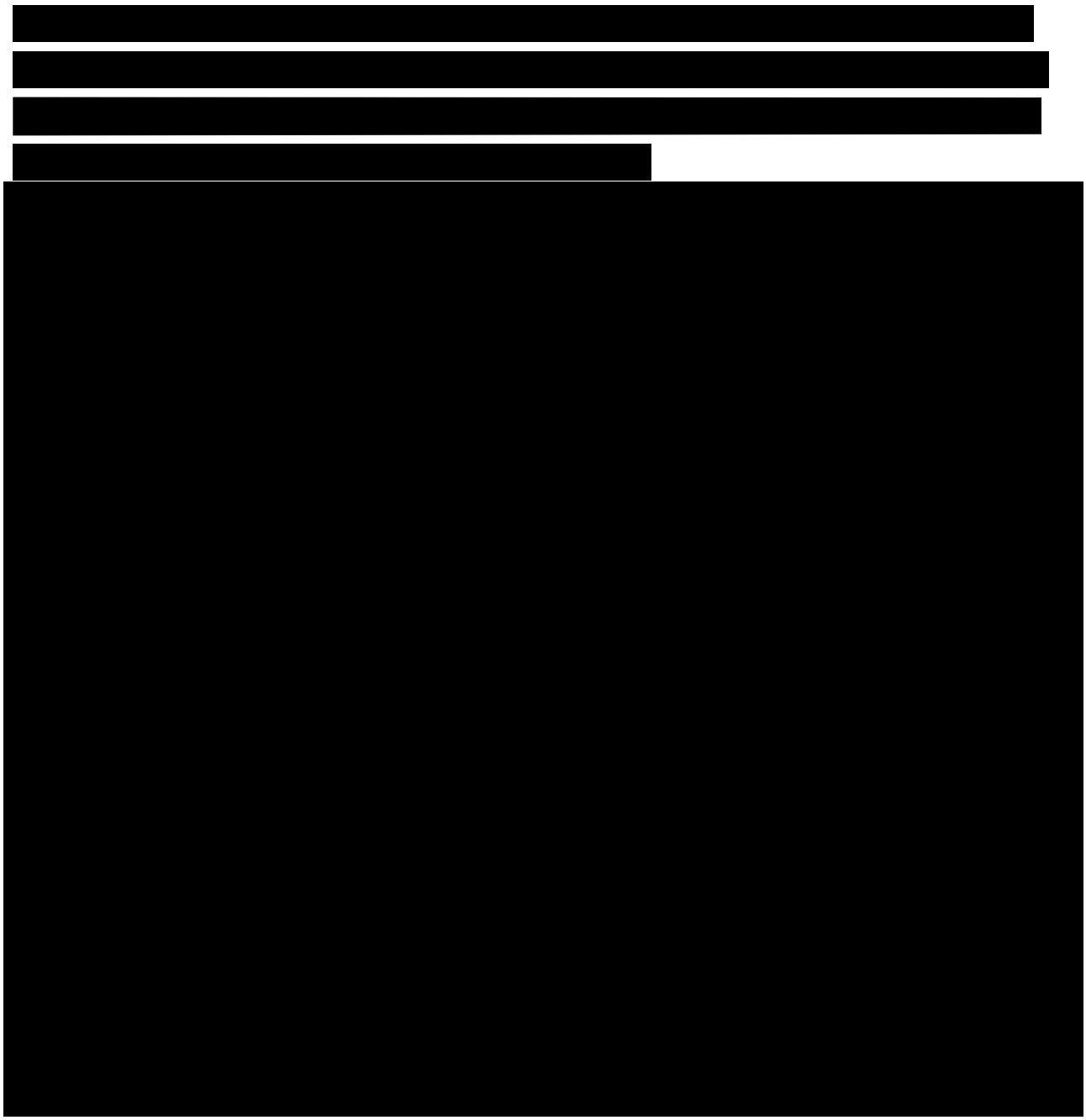


Exhibit 1-4. MetTel Network Architecture

Point of Presence (POP) Architecture

Exhibit 1-5. MetTel POP Architecture

Protecting Our Network

[redacted]

Agency Connections

[redacted]

MetTel's relationship with LECs, Tier-1 carriers, ISPs, wireless network and cable providers brings the most cost-effective AA to every connection. Having those relationships in place enables us to deliver quickly;

Exhibit 1-6. Customer Dedicated Connection Architecture

provides all the mandatory connection options at the Service Delivery Point (SDP).

Partner Networks

Networking has moved beyond single vendor dedicated access. Today, networks must be mobile and flexible to reach users when and where the Agency mission requires. MetTel POPs provide unrivaled connectivity to a abundance of carrier partners to offer substantial reach and performance from a single provider and management platform. provide multi-homed network connectivity. This approach enhances the security and resiliency of the network.

[redacted]

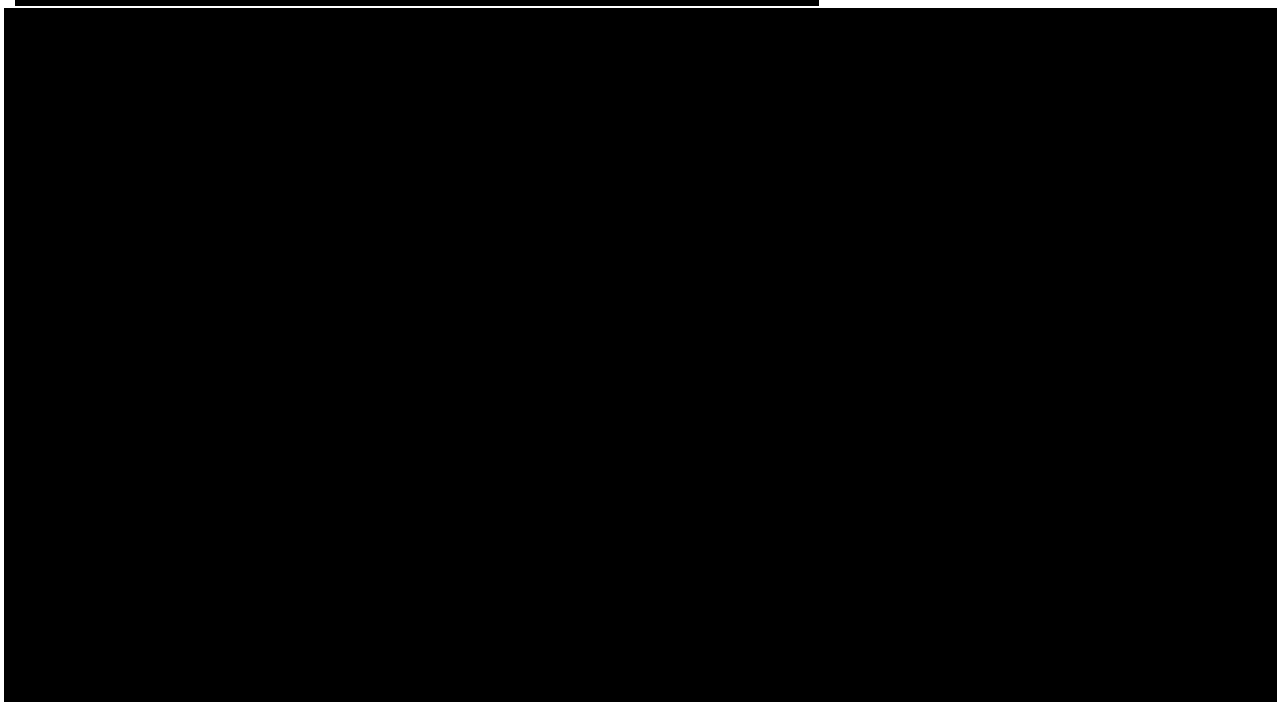


Exhibit 1-7. MetTel Network Access Architecture

POP Embedded Services Architecture

[redacted] to enable superior quality of experience for IP based services, the connectivity between the networks as shown above allows for shortest path access for all agencies. [redacted]

Exhibit 1-8. Embedded Services Architecture

Service Management Architecture

The MetTel EIS Portal provides a single interface into Billing, Services, Reporting, Ordering, and Help Desk information. This latest-technology implementation provides a resilient architecture that scales as the MetTel customer base expands. **Exhibit 1-9** illustrates the logical architectural overview of the MetTel EIS Portal.

Exhibit 1-9. MetTel EIS Service Management Architecture

[redacted] Easy-to-understand and comprehensive views of the Agency telecommunications spend allow for cost savings from proper cost allocation and focus on mission requirements.

MetTel EIS Portal Key Benefits

- Organized and manageable with automated invoice processing
- Keeps the Agency informed with dashboards, drill down, understandable reports

[redacted]

1.1.1 MetTel EIS Portal

The MetTel EIS Portal is central to the MetTel service management architecture.

[redacted] User access is based on user roles defined by the Agency [redacted] Agency access to the MetTel EIS Portal is established during the on-boarding process. MetTel and the Agency establish the proposed implementation plan and escalation roles and responsibilities. We provide training for Agency users and administrators. Staff authorized to order new services or add inventory to an existing service (i.e., adding phone lines) use the ordering functions shown in **Exhibit 1-10**.

[redacted]

Exhibit 1-10. MetTel EIS Portal Ordering Functions

Program Management

The MetTel EIS Portal supports the Program Manager and Agency [redacted]

[redacted]

Exhibit 1-11. MetTel EIS Portal Inventory Management

Trouble Ticket Management

The MetTel EIS Portal Trouble Ticket Management function supports the Agency and the help desk by creating and accessing Trouble Tickets and monitoring status. Trouble Tickets also track schedules for service installations and service repair, service testing, and billing. Over-the-Air (OTA) help desk provides Agency personnel the ability to open and manage tickets without contacting help desk staff. Real-time network maps with live and historic statistics are available to Agency users based on Agency authorization policy. [redacted]

Exhibit 1-12. Trouble Ticket Management

Network Monitoring and Management

This function provides the Agency access to MetTel's real-time monitoring on the MetTel EIS Portal. Agencies have

Exhibit 1-13. Network Monitoring and Management

Billing

The MetTel EIS Portal provides a complete consolidation of invoices and interactive analysis of current and historic charges. All bills are available in PDF/print format and EDI using X12 standard formats and other formats as specified by an Agency, including flat files to allow for streamlined upload to internal systems. MetTel's NCS team partners with the Agency to define the specific elements to be included in the electronic bill and implement the internal accounting structure throughout MetTel's billing system.

Exhibit 1-14. MetTel EIS Portal Billing Summary

MetTel provides comprehensive, flexible solutions designed to scale with Agency objectives. We have a demonstrated ability to consolidate and control telecommunications expenses for Government and large commercial organizations Our engineers and service management specialists provide the network resources and managed services specified in a Task Order and ensure Agency network services are cost-effective, compliant with EIS requirements, and manageable through the MetTel EIS Portal. We guide Agencies through every stage of transition, from mission inception to full operational capability on our industry-leading converged network.

Upgrades and Enhancements

MetTel embraces the evolution of technology to find the most effective and reliable

services for our customers. We were formed in 1996 to provide seamless, multi-carrier telecommunication services to leading commercial and Government organizations. We have effectively and efficiently deployed reliable, resilient traditional voice service to our expanding customer base. As convergence began to evolve in public and private IP networks, [redacted] We consider customer privacy and security a top priority and therefore security of our infrastructure and security monitoring are key components of our development. [redacted] The MetTel core network is the foundation for EIS services as well as the extension and deployment of upgrades and enhancements to our products and services.

[redacted] SD-WAN dramatically simplifies the customer's WAN by delivering virtualized services to branch offices and mobile users everywhere. MetTel leverages enterprise-grade performance, visibility, and control over both Internet and private networks. [redacted]

[redacted]

Managed Hybrid WAN

Public, private, and hybrid cloud services, mobility, machine to machine (M2M) unified communications/ collaboration, the Internet of Things (IoT), digital signage, ubiquitous Wi-Fi access, and other next-generation workloads require levels of bandwidth and availability beyond the capacity of legacy enterprise networks. [redacted]

MetTel Bonded Internet Service

MetTe [redacted]

[redacted]

MetTe [redacted] to better serve Agencies with expanded service. We continue to implement new and leading-technology services that enhance the Agencies experience, provide more effective network and bandwidth management, and provide cost savings and improved bandwidth utilization for our customers.

1.2 Quality of Services [L.29.1 (B), M.2.1 (2), C.1.8.2, C.1.8.3]

The MetTel solution for EIS is built on 20 years of experience as [redacted] in the market. MetTel established strong, sound, seasoned relationships with most of the local, national, and international providers to provide Government users with fully compliant services managed from a single source as well as, scalable, reliable, and resilient EIS services. [redacted]

We provide [redacted] The MetTel network accommodates and optimizes an Agency's

[redacted]

Exhibit 1-17. Example CoS Implementation

applications to ensure accurate and consistent prioritization of traffic across the network. [redacted]

Based on the agency's specified CoS definitions, the QoS mechanisms use these values to handle traffic in the communication path according to the Agency's defined policy. [redacted]

1.3 Service Coverage (for CBSA-dependent services) [L.29.1(C), M.2.1 (3), C.1.3, C.1.8.5]

The MetTel Network architecture enables the choice of lowest cost loops and access. [redacted]

Exhibit 1-18 shows that our services cover [redacted]

Exhibit 1-19. MetTel Global Network Reach

1.4 Security L.29.1(D), M.2.1(4)]

provide services and leadership end-to-end in cyber domain expertise, from mobile to cloud, from offense to defense, and from collection to analytics. MetTel delivers products, custom solutions, and supporting technologies to address a variety of Cyber missions and needs.

MetTel

This starts with policies, procedures, and security awareness campaigns. This is followed by the physical protections of our data centers and corporate offices to protect Agency information and assets as well as MetTel equipment.

The MetTel network protections start at our perimeter with our firewalls (described in further detail below) in fully redundant configurations. These protections deny by default any traffic not permitted on the MetTel network. [redacted]

Policies, Procedures, and Awareness

To protect our infrastructure resources, we developed a comprehensive series of security policies and procedures, [redacted] Our rigorous awareness and training program ensures our security staff is well equipped to manage today's complicated cyber-threat environment. Regular training and exercise is a mission-critical component of our security methodology.

Physical Defenses

[redacted]

Internal Network

Like all enterprises, insider threat is the single greatest threat to MetTel's internal network. We counter insider threats by performing enhanced background examinations of our staff members and following the Federal background investigation protocol specified in the GSA EIS RFP. [redacted]

Servers

[redacted] All unauthorized access attempts are highlighted in the log analysis report and immediately investigated.

2. TECHNICAL RESPONSE [L.28.2]

MetTel
Small Company Big Reach

- Advanced Facilities based MPLS Network
- Global MPLS reach
- Distributed Customer Care Centers
- MetTel EIS Portal for secure management
- Large choice of access providers
- Local Telephone Number footprint
- [redacted]

Since 1996, MetTel has been a strategic partner providing a comprehensive suite of voice and data solutions as well as telecom consulting services to leading businesses and government entities. From traditional voice services to MPLS networks and Voice over IP technologies, MetTel offers a complete portfolio of products. We achieve significant operational and cost efficiencies by leveraging our state-of-the-art back office infrastructure, sophisticated online MetTel EIS Portal, and international footprint.

MetTel Value

Our mission is to deliver value to our clients through unwavering commitment to:

✓ **Competitive Pricing**

- Significant Total Cost of Ownership savings
- Adherence to contracted rates and formal bill reviews
- Detailed billing and comprehensive reporting available via the MetTel EIS Portal

✓ **Superior Client Service**

- A single-point-of-contact within our Dedicated Care Team to ensure the prompt resolution of service matters
- Dedicated project management [redacted]
- Industry leading engineers designing scalable telecom platforms

✓ **Product Excellence**

- Innovative customized telecom solutions
- Integrated suite of traditional and advanced voice and data services
- Comprehensive telecom management consulting services

Track Record of Success

MetTel has been providing innovative, integrated communications solutions to customers across all industries since 1996. We redefine telecommunications by tailoring our products to provide cutting-edge solutions. [redacted]

[redacted]

Our Reach

MetTel brings the security of using the most trusted carriers in the country with the convenience of using one provider as the single point-of-contact in the United States. Our centralized customer care structure ensures standardized processes regardless of product class or geography. [redacted]

Our ability to meet GSA's present requirements and address the government's future telecom business needs have been demonstrated extensively in the private and public sector.

2.1 EIS Services [L.29.2.1, M.2.1, C.1.2, H.16; H.17; H.18; H.20; H.24]

MetTel will provide the EIS Mandatory and Optional services as specified in C.1.8.1 of the RFP and listed in **Exhibit 2.1-1.** All services proposed by MetTel are grouped by Service area and listed by RFP classification as mandatory or optional. Each service is defined in the referenced sections of this proposal.

Exhibit 2.1-1. MetTel EIS Proposed Services

[redacted]

[redacted]

Customer Technical Support

MetTel will provide customer technical support as a component of each of its EIS services. MetTel establishes and maintains strong relationships with our customers. We were awarded the prestigious Stevies Award for Outstanding Customer Service Department and Front-Line Customer Service Team in 2015. This award demonstrates our performance in providing reliable, flexible technical support at the highest levels.

We adapt and customize our solutions to customers' needs and ensure our customers obtain the best possible solution at the most competitive price. Our customer service and commitment to ensuring support distinguish our solutions from those of other offerors. [redacted]

[redacted]

We developed our service assurance processes from 20 years of experience serving commercial customers. Our processes represent industry best practices and include trouble ticket management. [redacted] We have gained considerable experience in meeting Government and Agency-specific requirements in connection with trouble ticket management using the MetTel EIS Portal as the interface for GSA and Agencies. Should escalations be required there are agreed upon escalation triggers and levels so GSA or the Agency always know who to contact if their operations require escalated support.

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.

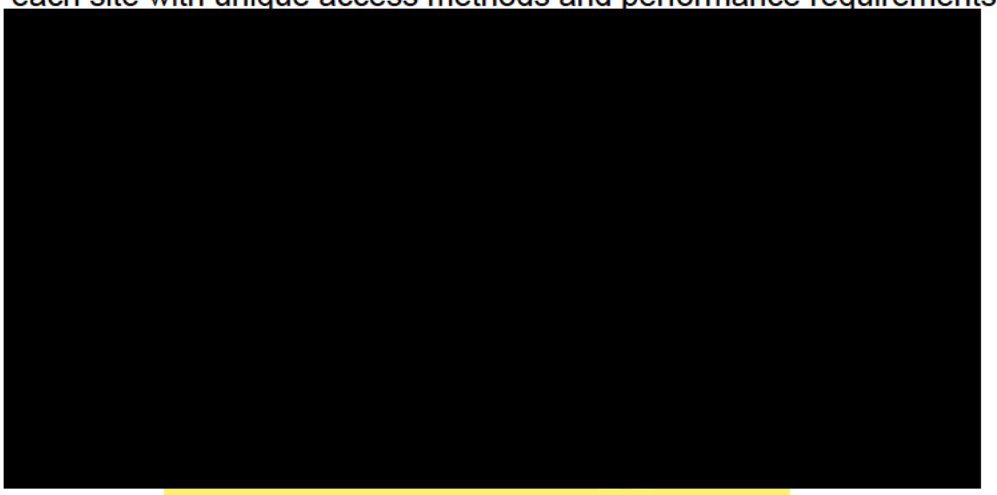
2.1.1.1.1 Service and Functional Description [L.29.2.1, C.2.1.1.1, C.2.1.1.1.1]

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] 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

[redacted]

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. [redacted]

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**

[redacted]

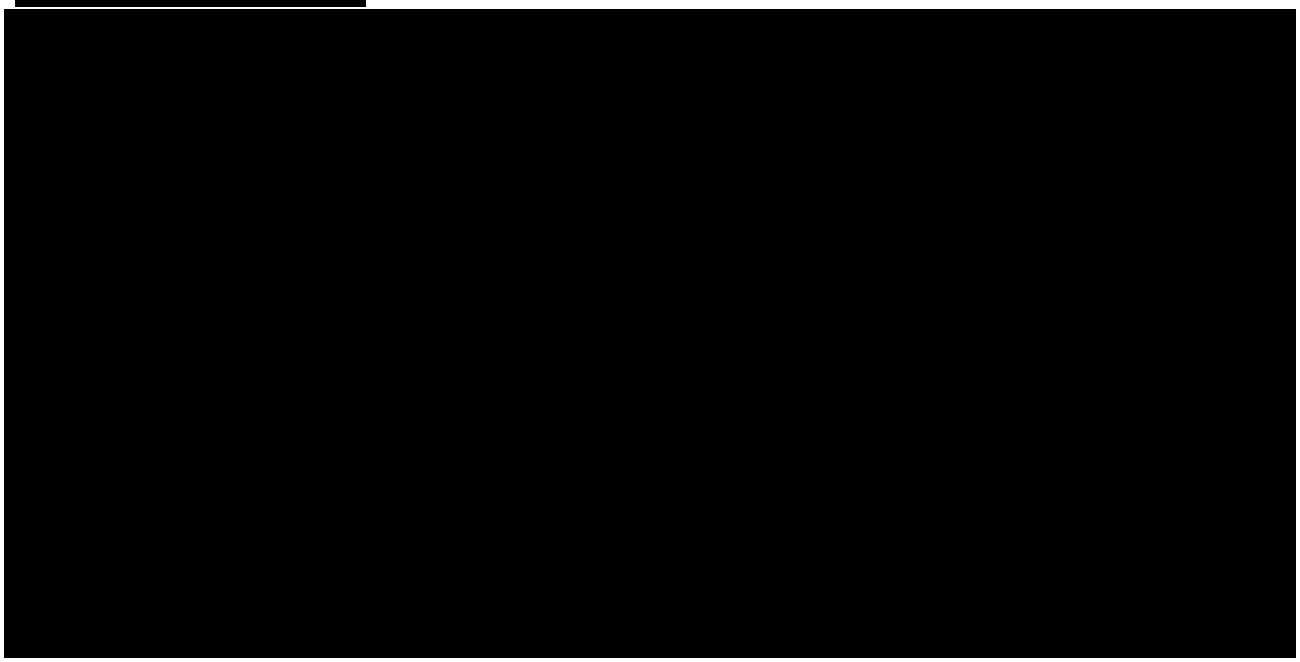


Exhibit 2.1.1-9. Load Sharing Configurations for VPNS

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.

2.1.2 Ethernet Transport Service [C.2.1.2]

MetTel Ethernet Transport Flexible Options
• Carrier Grade Transport Service • Ethernet over MPLS core backbone • Extensive global reach with partner providers • Many options for access • Bandwidth on demand to meet operational requirements

MetTel offers a fully compliant Carrier Grade Ethernet Transport Service (ETS) implemented over the MetTel core MPLS backbone. Ethernet links are transported using MPLS Label Switched Paths (LSPs) inside an outer MPLS tunnel. The MetTel core network is extended using network-to-network interfaces (NNI) to partner with providers to extend reach and provide connectivity options and alternative pricing approaches. With our extensive set of ETS last mile providers, MetTel exceeds the reach and connection options available on the network of any single provider. Using a combination of fiber, copper, cable, LECs and wireless provides the best opportunity to provide the most competitive price at any given location to meet service requirements.

2.1.2.1 Compliance with Evaluation Criteria [L.29.2.1]

The MetTel ETS solution fulfills the mandatory service requirements in SOW paragraph C.2.1.2. This section presents a technical description of our offering, demonstrating our capabilities in Standards, Connectivity, Technical Capabilities, Features, Performance Metrics, and Security. **Exhibit 2.1.2-1** highlights some key strengths and benefits of our ETS solution in relation to RFP Section M.2.1 evaluation criteria.

Exhibit 2.1.2-1. Features and Benefits of MetTel's Approach to ETS

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• ETS is a foundation service of MetTel's network and the preferred access method to the MetTel core network • Multi-network provider Ethernet NNI provides the widest choice of service and cost per geographic area • MEF 2.0 certified network partners • Eliminates the constraints of a single provider or single hardware vendor
Quality of Services (M.2.1(2))	• Full compliance with all SOW performance metrics including Availability, Latency, Jitter, Packet Loss, Packet Delivery, and Time-to-Restore • All KPIs available on the secure MetTel EIS Portal with current and historical reporting • 24x7 live customer support and service monitoring • [redacted]
Service Coverage (M.2.1(3))	• MetTel ETS rides on a nationally distributed network, with integrated strategically

Evaluation Criteria	Features and Benefits of MetTel's Approach
	dispersed communications switches, switching centers, and dedicated network links to eliminate latency issues and service interruptions • Ethernet NNI partners that extend the reach to more areas than are available from any single provider network • [redacted]
Security (M.2.1(4))	• Privacy and security is compliant with IEEE 802.3 and supported as defined in an Agency Task Order • ETS is provided over the MPLS core using industry-standard telecommunications facilities and equipment. • MetTel's network architecture ensures that an Agency's traffic is properly identified, routed (redirected), scanned (via secure DHS EINSTEIN Enclaves), and delivered to the appropriate Agency's 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 and reported in accordance with the EIS RFP. • MetTel supports the proper safeguards for handling 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.

2.1.2.1.1 Service and Functional Description [L.29.2.1, C.2.1.2.1, C.2.1.2.1.1]

Ethernet Transport Service MetTel Reach
• Multiple last-mile provider • Many different access technology choices • Cost-effective solution choices • MEF 2.0 standards based Ethernet

MetTel provides cost-effective, global Ethernet Service to EIS customers. Our multi-network Ethernet NNI enables us to extend an Agency's Ethernet wherever required to meet mission needs and security requirements. With this approach, we have eliminated many of the constraints of a single provider, single access provider, or single hardware vendor. We have the freedom to select the most cost-effective and/or most technically-appropriate solution based on the location, bandwidth, and survivability requirements. MetTel Ethernet will be provided as a dedicated service or a shared service.

[redacted] Our service delivery platform is extended as necessary to the leading MEF 2.0 certified vendors to expand our Ethernet Service to a large footprint [redacted]

Exhibit 2.1.2-2. Ethernet Service Architecture

Exhibit 2.1.2-2 shows our layered network architecture that provides global reach and service conformance. Our vendor arrangement with MEF CE 2.0 certified carriers provides unparalleled reach and capacity worldwide. The MetTel ETS provides a seamless end-to-end service from the SDP with the appropriate SRE, across the most direct network connection. This includes Metro access, Metro Core, Long Haul, or the extended MetTel backbone using the best choice Multi-Network Ethernet NNI. MetTel's approach is standards-based and does not require protocol conversion. If protocol conversion is required, we will specify the performance impact of delivering the service end-to-end.

We provide ETS over partner SONET networks and the extended MPLS backbone described above. Ethernet Services provide point-to-point, rooted multipoint, and multipoint-to-multipoint (fully meshed) connections. Ethernet provides a cost-effective, flexible, and robust connection that supports a combination of features that enable the transport of data with minimal protocol translation while supporting CoS and QoS across the network. We provide the following Ethernet services as defined by the MEF CE 2.0 and associated standards.

Ethernet Private Line (E-Line). E-Line is a point-to-point service that connects Agency sites with reserved bandwidth for mission-critical applications. MetTel implements E-Line service using our MPLS core and the Ethernet NNI. The Ethernet NNI provides industry-standard Ethernet extensions with vast global reach and connectivity. We provide connectivity across the MAN or WAN. E-Line supports full port speeds (10 MB, 100 MB, 1 GB, and 10/40/100 Gbps or higher Gbps) ports as they are available by location (i.e. CBSA). E-Line supports different QoS priorities for customer traffic and meets the KPIs specified in C.2.1.2.4. We deliver E-Line services in the most economical means using the best partner NNI or our MPLS backbone. **Exhibit 2.1.2-3** shows the connection of on-net and off-net sites with E-Line.

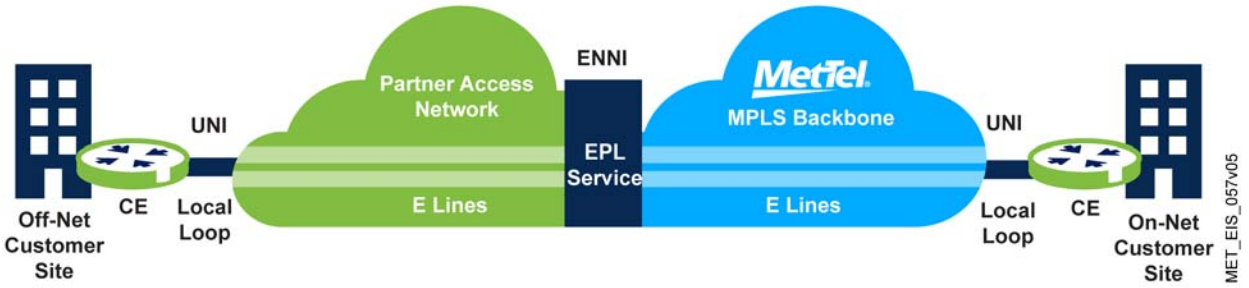


Exhibit 2.1.2-3. E-Line Extended Delivery Model

Ethernet Private LAN (E-LAN). Our E-LAN service supports both point-to-multipoint and fully meshed configurations. For point-to-multipoint service, E-LAN connects three or more sites over Layer 2 tunnels across MetTel or partner MPLS networks. We support ports of 10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 or higher Gbps as available by location (i.e. CBSAs), and QoS is supported for prioritizing customer traffic. For fully meshed configurations, E-LAN connects one or more roots and a set of leaves but to ensure confidentiality of agency traffic will deny inter-leaf communications. Multiple sites can be configured as the root site, and other sites can communicate with each other through multiple root sites. Thus Agencies connect disparate LAN segments into a single Agency-wide or inter-Agency virtual LAN that can span a MAN and/or a WAN. **Exhibit 2.1.2-4** shows the connection of on-net and off-net sites with E-LAN.

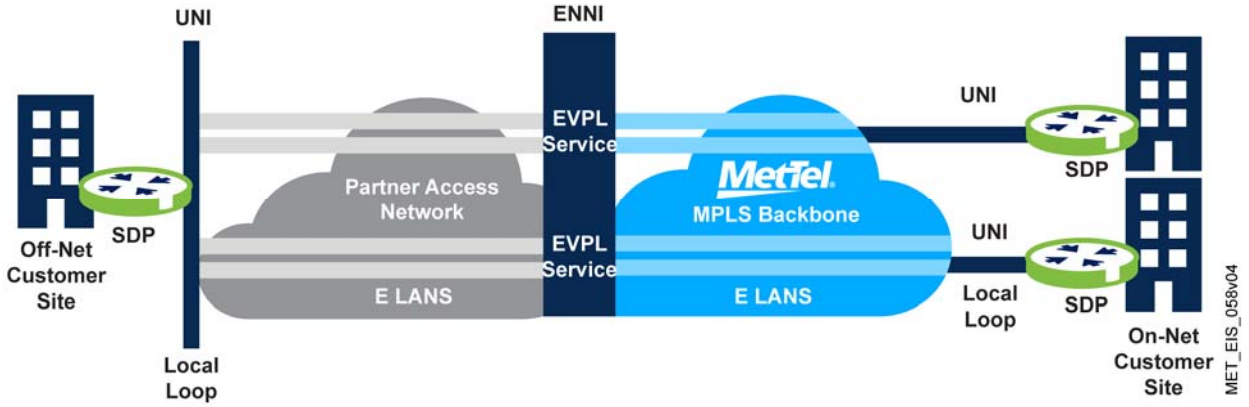


Exhibit 2.1.2-4. E-LAN Extended Delivery Model

Our ETS is engineered, monitored, and managed end-to-end to ensure compliance with all requirements specified in the specific Agency Task Order. We provide the capacity and bandwidth to transport the Government's information and conform to the Metro Ethernet Forum MEF CE 2.0, IETF RFC 3069, ITU standards for Network Architecture, Services, Operations and Maintenance (O&M), Protection, Equipment, and Equipment Management and Terminology. We also conform to IEEE Standards and Acceptance Testing of Ethernet Service as defined in C.2.1.2.1.2 of the EIS RFP. We support new versions as other standards evolve or these are updated.

2.1.2.1.2 Standards [L.29.2.1, C.2.1.2.1.2]

Carrier Ethernet (CE) 2.0 provides a global standard for service providers to interconnect more quickly and meet the growing needs for Carrier Ethernet services at locations not on a service provider's own network. Such locations are referred to as off-net. This standard provides the mechanism and standard interface to our Multi-Network Ethernet NNI. Exhibits 2.1.2-2 and 2.1.2-3 show the approach to providing both E-Line and E-LAN.

Our partners are the leaders in Ethernet delivery and Ethernet standards development. **Exhibit 2.1.2-5** is a partial list of our partner providers and their current MEF certification. Most of our partners are MEF CE 2.0 certified, a strength in our delivery of standards-compliant ETS. We deliver Ethernet services compliant with all the standards defined in C.2.1.2.1.2. [redacted]

Exhibit 2.1.2-5. MetTel Ethernet Partner Service Providers

2.1.2.1.3 Connectivity [L.29.2.1, C.2.1.2.1.3]

Our ETS provides connectivity and interoperates with:

1. Intra-agency LAN-LAN Connectivity. Ethernet Service provides connectivity for LAN implementations located in the same or different metropolitan areas. This enables the Agency to extend the LAN to the MAN or WAN by connecting the Agency's SDP(s) in one location to another SDP(s) in one or more locations. Interconnections are possible over transoceanic links if required.
2. Inter-agency LAN-LAN Connectivity. When different Agencies share resources to connect to the contractor's metro or long-haul network, we connect one Agency's SDP(s) to the other Agency's SDP(s).

2.1.2.1.4 Technical Capabilities [L.29.2.1, C.2.1.2.1.4]

The MetTel architecture allows Agencies to interconnect their LANs transparently over MAN and WAN regardless of the geographic diversity of their sites. **Exhibit 2.1.2-6** defines our response to all ETS technical capabilities in the EIS RFP.

Exhibit 2.1.2-6. Ethernet Transport Service Technical Capabilities

C.2.1.2.1.4 Reference	Feature	MetTel Response
1	Routing Requirements (C.1.8.8)	MetTel's network architecture and security partner Raytheon, ensures that Agency traffic is properly identified, routed (redirected), scanned and monitored (via EINSTEIN enclaves), and delivered to the appropriate Agency network. Our architecture also enables us to identify any traffic that has been inadvertently directed though the DHS EINSTEIN enclave and notify DHS. Metrics (SLA KPIs) are measured in accordance with the EIS RFP.

C.2.1.2.1.4 Reference	Feature	MetTel Response
		MetTel team supports the proper safeguards for handling traffic should failures occur with the DHS GFP. Additionally, all DHS EINSTEIN enclaves are housed within a planned ANSI/TIA-942 and ICD 705 certified facility.
2	Geographic Coverage	The MetTel architecture provides Agencies a seamless end-to-end service from the SDP SRE (CPE) over Metro Access, MetTel core MPLS network and across NNIs which minimizes conversions of protocols. If protocol conversions are required, MetTel identifies how they will impact service delivery. MetTel provides Ethernet connections (Intra-city ETS) to Agency sites located in the same city in the continental U.S. (CONUS) and outside the continental U.S. (OCONUS). ETS provides connections at both domestic and non-domestic locations.
3	Support Layer 2 and 3 Clients	MetTel's Ethernet service is delivered via a User-to-Network-Interface (UNI) at the Agency SDP and supports Layer 2 (i.e. Switches) and Layer 3 clients (i.e. Routers); this includes Agency clients that support Layer 3 protocols such as IPv4 and IPv6.
4	Ethernet Virtual Connections (EVC)	MetTel's ETS operates over EVCs, which provides the association of two or more UNIs.
5	ETS Delivery	MetTel delivers ETS service to an Agency SDP via a UNI.
6	Circuit Emulation	Should it be required, MetTel will support circuit emulation services for TDM transport.
7	EVC Support	MetTel supports point-to-point, multipoint-to-multipoint, and Rooted multipoint EVCs.
8	EVC Multiplexing	MetTel supports EVC multiplexing
9	Rate Limited Throughput Access Links	MetTel supports rate-limited throughput access links. For example, a 100 Mbps port can be limited to 40 Mbps, or a 1 Gbps port can be limited to 200 Mbps. Increments for rate limiting are 1 Mbps on a 10 Mbps port, 10 Mbps on a 100 Mbps port, and 100 Mbps for a 1 Gbps port.
10	Rate Limiting at SDP	MetTel supports rate limiting at the Agency SDP and at the individual VLAN ingress and egress.
11	Privacy and Security	MetTel supports security as defined in IEEE 802.3 as defined in the Task Order.
12	Physical Interfaces	MetTel supports the physical interfaces defined in C.2.1.2.3 for all the mandatory interfaces as descr bed in Section 2.1.2.6.
13	Traffic Profiles	MetTel supports the following traffic profiles, called Bandwidth Profiles by the MEF: Committed Information Rate (CIR) Committed Burst Size (CBS) Peak Information Rate (PIR) MBS – Often called the burst information rate and is equal to the maximum information rate at which bursts can be sent.
14	Performance Metrics	See Section 2.1.2.1.7
15	Service Frame Delivery	MetTel provides Service Frame Delivery options that include Unicast Frame Delivery, Multicast Frame Delivery (RFC 4604), and Broadcast Frame Delivery (IEEE 802.3)
16	VLAN Tag Support	MetTel provides support for Virtual LAN (VLAN) tags for preservation, translation, and stacking, defined in IEEE 802.1Q.
17	Service Multiplexing	MetTel supports multiple EVCs connected via a single UNI.
18	Bundling	MetTel supports bundling to enable two or more VLAN IDs to be mapped into a single EVC at a UNI.

C.2.1.2.1.4 Reference	Feature	MetTel Response
19	Security Filters	MetTel supports security filters as defined by an Agency Task Order. Notification of triggered filters are sent to the SOC.
20	Performance Monitoring	[redacted]
21	Maintenance Functions	MetTel has a full set of network maintenance functions defined by the MPLS-TP O&M standards efforts and supports EIS maintenance. These include: Alarm Suppression: the ability to turn off an alarm to enable problem or transmission analysis. Loopbacks: primarily a means of testing the transmission infrastructure. Can be accomplished in intrusive or non-intrusive (transparent to on-going connections) mode. Protection switching and restoration, [redacted]
22	Network Topologies	MetTel supports the implementation of point-to-point, rooted multipoint, and multipoint-to-multipoint (mesh) network topologies.
23	Geographical Diversity	MetTel provides geographically diverse connections to provide added reliability. Agencies can buy geographically diverse routes from MetTel or a different provider to serve as a protection path. MetTel provides both paths to ensure geographical diversity as a partner provider and provides the second path and connect through the ENNI. Refer to Access Arrangements in Section 2.1.5 for a full description of diversity options.
24	Bridging	MetTel supports bridging, which is the connection of a LAN to another LAN that uses the same protocol; in the EIS case, this is Ethernet. IEEE 802.1X-REV is a revision of the IEEE 802.1X standard that contains security encryption and secure key exchange, allowing secure communication between authenticated and authorized devices. The 802.1X-REV feature includes the 802.1AE MAC Security (MACSec) encryption as well as 802.1af, MACSec Key Agreement (MKA) protocol.
25	Virtual Connection Sizes	MetTel supports Virtual Connection sizes for point-to-point and multipoint-to-multipoint Ethernet connections up to 40 Gbps.
26	Quality of Service (QoS)	MetTel provides QoS and traffic prioritization that enables higher priority traffic to be transmitted first. The MetTel network accommodates and optimizes an Agency's applications to ensure accurate and consistent prioritization of traffic across the network.
27	Traffic Reconfiguration	MetTel Customer Support is flex ble and able to modify a specific service connection after the connection is established. Changes to an established connection may include an upgrade or downgrade of speeds that do not result in physical equipment changes.

2.1.2.1.5 Features [L.29.2.1, C.2.1.2.2]

Reserved

2.1.2.1.6 Interfaces [L.29.2.1, C.2.1.2.3]

We provide UNI Types 1, 2, 14, and 15 as required by EIS RFP Section C.2.1.2.3.

[redacted]

2.1.2.1.7 Performance Metrics [L.29.2.1, C.2.1.2.4]

Our embedded performance collection and management capabilities provide real-time and historic reporting of the AQL of KPIs for the ETS. [redacted] The Trouble Ticketing element of the MetTel Portal maintains and reports time-to-restore which is also used by the SOC for correlation and analysis of events.

2.1.3 Internet Protocol Voice Service [C.2.2.1]

MetTel IPVS
Foundation for Communication

- Integrated in the MetTel MPLS core network with full redundancy at multiple geographically diverse secured locations
- Multiple diverse connections to the PSTN

MetTel provides a fully compliant Internet Protocol Voice Service (IPVS) built on a MetTel-owned network of [redacted] Agencies leverage all the functionality of a large enterprise phone system while saving time and money with the network-based IPVS. IPVS provides an effective migration path from premise based systems and traditional PSTN interfaces such as PBXs to a full IPVS or an integrated solution that uses both traditional telephone systems and IPVS. We combine simplified calling plans with advanced IP features to enhance Agency call quality and productivity. Our IPVS provides full functionality and connectivity using the MPLS core network, high-speed connections to major PSTN providers and wireless networks.

[redacted] We coordinate project planning and implementation with the Agency to ensure timelines are met and the IPVS implementation is seamless and integrated into the telecommunications infrastructure without interruption to operations.

[redacted]. Our MetTel EIS Portal is based on our commercial portal, Bruin, which was recently awarded the **2016 Internet Telephone Product of the Year**. TMCnet recognized and awarded MetTel for having developed exceptional VoIP and IP Communications products and services. Using our Portal, Agencies have total access to the self-provisioning option, inventory, implementation planning and schedules, performance reporting, trouble ticket management, and billing.

2.1.3.1 Compliance with Evaluation Criteria [L.29.2.1, M.2.1]

The MetTel IPVS solution meets the mandatory requirements in SOW paragraph C.2.1.1. This section presents a technical description of our offering, demonstrating our capabilities in Standards, Connectivity, Technical Capabilities, Features, Performance Metrics, and Security. **Exhibit 2.1.3-1** highlights some key strengths and benefits of our IPVS solution in relation to RFP Section M.2.1 evaluation criteria.

Exhibit 2.1.3-1. Features and Benefits of MetTel's Approach to IPVS

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	[redacted] • MetTel's secure and dedicated SIP trunks to major PSTN and wireless providers • MetTel EIS Portal for Agency control and management of telecommunications expenses • MetTel IPVS is simple to configure and maintain. No hidden costs with the deployment and management of hosted users • Fully managed migration from CSVS to IPVS to move Agencies into the converged networking environment • Professional installation and management with Managed LAN Service
Quality of Services (M.2.1(2))	• Careful monitoring and management of technology scaling issues to ensure IPVS [redacted] • Built-in resiliency with dynamic rerouting of calls in the network • 24x7 live customer support and service monitoring • Timely access to secure MetTel EIS Portal for self-provisioning option, inventory management, performance management, quality management with real-time and historic data displays, and drill down to circuit, site, or phone number.
Service Coverage (M.2.1(3))	• IPVS that rides on nationally distributed MetTel network, with integrated strategically dispersed communications switches, switching centers, and dedicated network links to eliminate latency issues and service interruptions [redacted] • Full-support E911/911 service with the location of the originating device routed to the appropriate Public Safety Answering Point (PSAP)
Security (M.2.1(4))	• Compatible with Agency firewalls and security layers with minimal port and service exposure for IPVS • Regularly updated and audited security practices and policies [redacted]

2.1.3.1.1 Service and Functional Description [L.29.2.1, C.2.2.1.1, C.2.2.1.1.1]

MetTel IPVS
Global Reach

- Cost Savings
- Simplified Agency Moves, Adds, and Changes with Agency option to self-provision through the MetTel EIS Portal
- Customizable extension dialing plans
- Many options for devices, VoIP, and Analog
- Increased flexibility and scalability
- Easy web-based management through MetTel EIS Portal
- Improved Business Continuity and Disaster Recovery (DR)
- Many included features

MetTel's IPVS provides support for voice calls initiated from on-net or off-net locations to be connected to all on-net and off-net locations by direct dialing. MetTel IPVS has global termination through its strong partnership with the major national and international PSTN access providers. IPVS provides a network-based solution implemented in the MetTel MPLS core network. IPVS also provides premises-based telephone service over the MetTel IP network. Support for IPVS includes Managed LAN Service for implementation and management of the Agency premise environment to connect IP devices and analog devices to IPVS. Session Initiation Protocol (SIP) trunk service is provided to interoperate with any Private Branch Exchange (PBX) system that supports SIP-based IP trunk interfaces.

[redacted]

MetTelt provides user services, administrative features, and media-based functionality from a standards-based service delivery platform that operates on a modular architecture that uses common protocols (such as SIP), open interfaces, and scalable, industry-standard hardware. [redacted]

[redacted]

[redacted]

MetTel IPVS satisfies all the requirements of EIS RFP Section C.2.2.1. IPVS is embedded in our MPLS core network and extended through direct connections to all the major PSTN access providers. We manage the converged MPLS IP core network to provide service in compliance with all KPIs. **Exhibit 2.1.3-3** shows MetTel IPVS phones and analog telephone adapters connecting over the QoS enabled MetTel network,

which connects calls on-net, off-net, and over the PSTN.

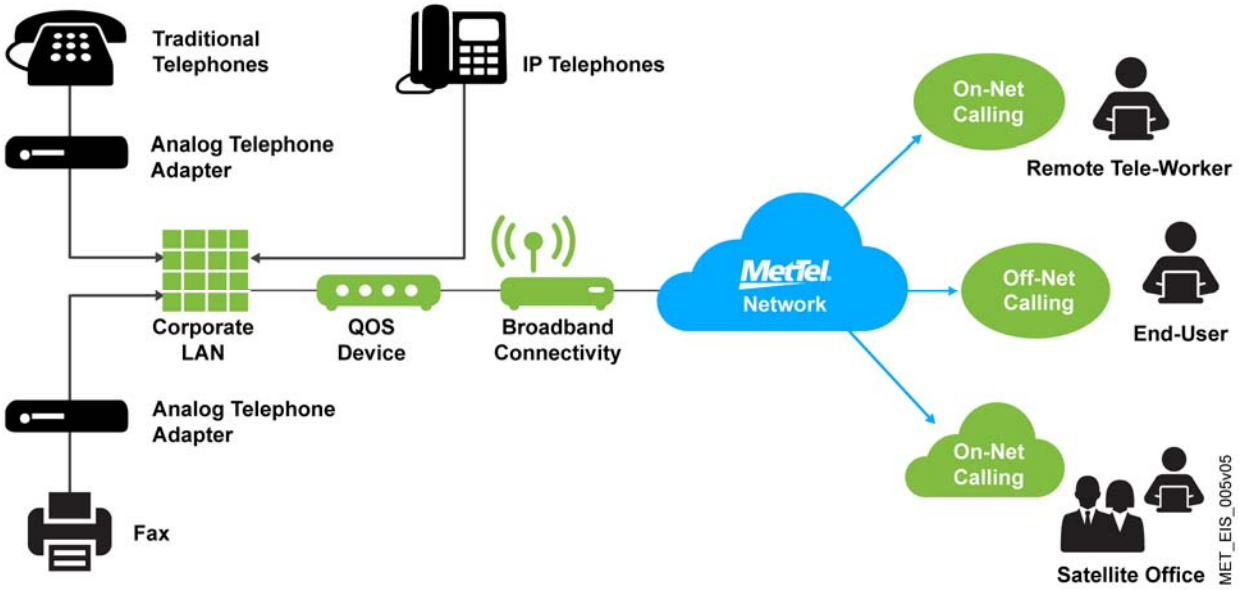


Exhibit 2.1.3-3. MetTel Converged IPVS

MetTel IPVS has global termination reach through strong partnerships with the major national and international PSTN providers. High-speed SIP trunks to these providers enable us to reach any number in CONUS or OCONUS. As shown in **Exhibit 2.1.3-4**, our core network is extended to providers with connectivity worldwide.

Exhibit 2.1.3-4. Global Reach for IP Voice Services

2.1.3.1.2 Standards [L.29.2.1, C.2.2.1.1.2]

MetTel IPVS interoperates with the PSTN, wireless, and international networks and complies with ITU-T G.711, ITU-T H323, H.350 codecs, Real-time Transport Protocol (RTP) IETF RFC 3550, and SIP IETF RFC 326. [redacted]

2.1.3.1.3 Connectivity [L.29.2.1, C.2.2.1.1.3]

MetTel was founded as a CLEC and migrated to a facilities-based telecommunications integrator. MetTel takes specific steps to ensure traffic is given the appropriate priority to traverse the network to stringent QoS standards [redacted]

MetTel IPVS connects and interoperates with the PSTN (wireline and wireless networks) CONUS and OCONUS and is built on our MPLS core network with embedded [redacted] The network extends to the major PSTN providers to enable telephone numbers and traffic to spread over multiple carriers. **Exhibit 2.1.3-5** shows how our core network interacts with multiple PSTN providers and wireless networks.

Our IPVS connects and interoperates with other EIS contractors' voice service networks and satellite-based voice networks in both domestic and non-domestic locations using the interconnections with the PSTN. MetTel IPVS supports voice calls from anywhere to anywhere whether initiated from on-net locations, off-net locations, wireline or wireless, or satellite by the most direct route through the MetTel network. MetTel IPVS is standards-based and complies with required standards in RFP Section C.2.2.1.1.2.

Exhibit 2.1.3-5. MetTel Voice Architecture

2.1.3.1.4 Technical Capabilities [L.29.2.1, C.2.2.1.1.4]

The MetTel IPVS is fully compliant with the technical capabilities defined in C.2.2.1.1.4, as shown in **Exhibit 2.1.3-6**. The IPVS includes unlimited on-net to on-net and on-net to CONUS off-net calling. The IPVS supports off-net calling to CONUS, OCONUS, and the Non-Domestic locations shown in RFP J.1.2.

Exhibit 2.1.3-6. MetTel IPVS Technical Capabilities

Technical Capability	Implementation
Remote Access	The Remote Office Access service enables users to access and use their IPVS from any end point, on-net or off-net (e.g., home office, mobile phone). This service is especially useful for telecommuters and mobile workers as it enables them to use all of their web features while working remotely (e.g., extension dialing, transfers, conference calls, Outlook integration, directories, etc.).
(1) Real-time Transport	MetTel's IPVS provides transport for voice, Fax, TTY communications and data.
(2) Real-time Delivery of Caller ID (ANI)	An incoming call with an associated caller ID (ANI) is displayed on the subscriber device, based on the capability of the device.

Technical Capability	Implementation
(3) Interoperate – Public	MetTel's IPVS interoperates with public network dial plans (North America Numbering Plan), Direct Inward Dialing (DID) service through one of multiple PSTN providers and ITU-T E.164 that defines a numbering plan for world-wide PSTN and other data networks.
(4) Interoperate – Private	MetTel's IPVS supports private and customizable network dial plans and direct dialing.
(5) Interoperate – Non-Commercial (Optional)	MetTel's IPVS interoperates with non-commercial, Agency-specific NPA 700 through the PSTN.
(6) Public Directory and Operator Assistance	MetTel's IPVS provides access to public directory by dialing 411. Operator assistance is available for the public directory by dialing 411 and dialing 0 or the number specified in the auto attendant.
(7) Unique Directory Numbers	MetTel provides unique directory numbers for all on-net Government locations, including support for existing Government numbers.
(8) Automatic Callback	MetTel Call Return enables a user to call back the last party that called by dialing the call recall star code. Users can also execute call recall via the portal.
(9) Support Three-way Calling	IPVS supports a three-way call with two other parties using device features or portal features.
Gateways for Interoperability	IPVS provides two types of gateways between the IP network and the PSTN or Agency UNIs. 1. MetTel provides the Subscr ber Gateways for interoperability to non-proprietary telephone devices, analog stations, and ISDN BRI station interfaces. 2. PSTN Gateways provide transparent access and interwork with the domestic and non-domestic PSTN. MetTel has multiple agreements with PSTN providers and access to multiple gateways through secure SIP trunks.
Station Mobility	IPVS provides IP subscr bers the ability to move IP phones within the Agency's enterprise-wide network and access IP services. This station mobility has a major impact on the reduction of cost associated with Moves, Adds, or Changes within an Agency.
Traverse Agency Firewalls	IPVS allows for implementation with Agency firewalls [redacted] MetTel verifies with the Agency that the Agency firewall is compatible with IPVS.
Security Practices and Safeguards	MetTel provides SIP gateways and SIP firewalls to protect the network from external threat. This includes: • **Denial of Service** – Safeguards prevent hackers, worms, or viruses from denying legitimate users from receiving quality, reliable, and resilient IP Voice Services. [redacted] • **Intrusion** – Safeguards are provided to mitigate attempt to illegitimate use of IPVS. [redacted] • **Invasion of Privacy** – Safeguards are provided to ensure IPVS is private and unauthorized third parties cannot eavesdrop or intercept IPVS phone numbers, IP addresses, or URLs. [redacted]

Technical Capability	Implementation
Unauthorized Access	[redacted]
Emergency Service Requirement	IPVS provides emergency services requirements, including 911 and E911 service, and identifies the location of the originating station and routes them to the appropriate PSAP.
Local Number Portability	Routing policy supports the porting of users on to and out of IPVS. MetTel fully complies with the FCC Local Number Portability requirements.

[redacted]

2.1.3.1.5 Features [L.29.2.1, C.2.2.1.2]

MetTel's IPVS provides a rich set of features and services, including Voicemail, Auto Attendant, and Augmented 911/E911 Service.

Voice Messaging and Voicemail Boxes [C.2.2.1.2 (1)]

Voicemail supports voice messaging transmission, reception, and storage. Callers may review and/or change their message and hear a warning tone when reaching the maximum message length.

From the MetTel EIS Portal, users control whether voicemail messages are delivered as .WAV attachments in email and/or to the system repository for retrieval from a phone. The web interface also enables users to enter their password and give callers the option of connecting to an attendant by pressing 0.

Users can record their name and multiple greetings using the Voice Portal and can access the Portal from any phone to listen to, save, and delete messages and mark them as Urgent or Confidential. During message playback, users may skip forward, skip back, pause, reply to and forward messages. Users can pre-configure lists of users to whom messages are sent and compose and forward messages with an introductory message to one or more group members or an entire group.

A feature access code allows users to send incoming calls directly to their mailbox or the mailbox of any other user within their group. [redacted]

MetTel IPVS provides the following additional voicemail features:

- **Immediate Voicemail.** Provides an "always on" voice mailbox. With the user's "number of rings before greeting" parameter set to "0," a caller is immediately provided the no-answer greeting and the user's device is not alerted.
- **Voice Message Waiting Indication.** Provides a stutter tone via the user's telephone when new messages reside in their voice mailbox. A visual indicator on the phone is also provided, if applicable.
- **Voice Message Notification.** Enables a user to be informed of new voice messages. The notification is in the form of an email (or short message to a cell phone) or an indication on the user's station. The user controls the service via a web interface, which provides the ability to activate and deactivate email notification as well as the email notification address.

Auto Attendant [C.2.2.1.2 (2)]

MetTel's Auto Attendant serves as an automated receptionist that provides options for callers to connect to an operator, extension or dial-by-name, various attendant positions, external phone numbers, mailboxes, or nine configurable options (e.g., 1 for Information, 2 for Account Information, etc.).

A group can have multiple Auto Attendants configured either individually (e.g., customer service with separate business hours) or integrated into a multi-level Auto Attendant (e.g., enterprise's main Auto Attendant is configured to seamlessly route to the Auto Attendant of a particular department or location).

Augmented 911/E911 Service [C2.2.1.2 (3)]

We will populate a 911 Private Switch/Automatic Location Identification (PS/ALI) database with the Government's profile, which includes all user telephone numbers,

station locations, building location, building address, building floor, room number, and geocode during service implementation. We provide secure remote Government access via a web browser to allow the Government to maintain the profile (e.g., to account for moves, adds, deletions, or other changes). We ensure these profile updates are reflected in the PS/ALI database. Our nationwide augmented 911/E911 service is supported 24x7x365 and provides multiple address validation sources, has bulk upload capability, and is FCC/CRTC compliant.

[redacted]

Standard Features

Exhibit 2.1.3-8 defines the standard features of our basic service and [redacted]

and comply with the technical capabilities defined in C.2.2.1.2.

Exhibit 2.1.3-8. IPVS User and Administrator Capabilities

Capability	Feature Description	[redacted]	[redacted]
(1) Calling Line ID Delivery	Displays a caller's identity to a user via the web interface and phone (if capable). Delivered information includes the caller's	[redacted]	[redacted]

Capability	Feature Description	[redacted]	[redacted]
	phone number and name. The information is delivered to the web interface and phone (if capable) only if the information is available and not blocked by the caller.	[redacted]	[redacted]
(2) Conference Calling	Enables a user to make a three-way call with two parties.		
(3) Do Not Disturb	Allows a user to set their station as unavailable. All calls are treated as busy.		
(4) Call Forwarding – All	Enables a user to redirect all calls to another destination.		
(5) Call Park	Enables a user to hold a call and retrieve it from another station within the group. Can also be executed via the web interface.	[redacted]	[redacted]
(6) Hotline	A Series Completion service that can be assigned to a selected series of lines to forward calls on a busy condition. A form of "hunting" in which the next line in the group is tried in a prearranged order, without any limit on the number of sequential forwards		
(7) Call Forwarding – Busy	Enables a user to redirect calls to another destination when an incoming call encounters a busy condition.		
(8) Call Pickup	Enables a user to answer any ringing line within their pick-up group, which is a group administrator-defined set of users to which the call pickup feature applies.		[redacted]
(9) Hunt Groups	Allows users within a group to be included in a specified sub-group to handle incoming calls received by an assigned Hunt Group phone number.	[redacted]	[redacted]
(10) Call	Enables a user to redirect calls to another		

Capability	Feature Description	[redacted]	[redacted]
Forward – No answer	destination when an incoming call is not answered within a specified number of rings.		
(11) Class of Service Restriction (CoSR)	Defines the restrictions that apply when a user places or receives a call. Allows or denies user access to some system features.		
(12) Multi-Line Appearance	Allows a line that is an address-of-record to place and receive calls on multiple end points.		
(13) Call Hold	Allows a user to place a call in hold status by pressing the appropriate button on the phone. Music on hold feature is also available.	[redacted]	[redacted]
(14) Distinctive Alert/Ring	Provides a different call waiting tone (i.e., alert) or a different ringing cadence for intra-group calls versus calls received from outside the group.	[redacted]	[redacted]
(15) Directory Assistance	Enables users to view and print a directory listing of all the Agency group members and their respective contact information (e.g., extension, phone number, email address).		
(16) Call Transfer	Enables a user to consult with the add-on party before transferring the caller	[redacted]	[redacted]
(17) Call Waiting	Enables a user to answer a call while already engaged in another call.		
(18) Speed Dial	Enables users to dial single digit codes to call up to eight numbers, such as frequently dialed numbers or long strings of digits that are difficult to remember.	[redacted]	[redacted]
(19) Call Number Suppression	Enables users to block their outgoing caller ID on a per call basis by dialing a star code before making the call		
(20) Specific Call Rejection	Enables a user to define criteria that causes certain incoming calls to be blocked. If an incoming call meets user-specified criteria, the call is blocked and the caller is informed that the user is not accepting calls.	[redacted]	[redacted]

Capability	Feature Description	[redacted]	[redacted]
(21) Last Number Dialed	Enables users to redial the last number they called by clicking the "Redial" button on their web interface or by dialing a feature code (e.g., *66).		
(22) IP Telephone Manager (Administrator)	A portal that allows Agency administrators to control and modify options such as automated attendant, music, on hold, etc.		
(23) IP Telephone Manager (Subscriber)	A portal that offers the IPVS user the ability to control and personalize their service. Voicemail delivery options, call forwarding, do not disturb, simultaneous ring, etc. are some of the options that can be configured.		

2.1.3.1.6 Interfaces [L.29.2.1, C.2.2.1.3]

The SRE catalogue lists multiple SREs to provide scalable solutions for routers and switches. All UNIs at the SDP support IEEE 802.3 with RJ-45 ports up to 100Mbps. [redacted]. All signaling is SIP (IETF RFC 3261, H.323, MGCP or SCCP).

All devices in the SRE catalogue are labeled for the interface they support. The devices that support IPVS all have in the Notes column, IPVS-1 to indicate they support UNI-1 as defined in EIS RFP Section C.2.2.1.3.

2.1.3.1.7 Performance Metrics [L.29.2.1, C.2.2.1.4]

MetTel has embedded performance management and reporting capability in the MPLS core network. For IPVS, we report latency, packet loss, availability, jitter, Mean Opinion Score (MOS) and Round Trip delay Time (RTT). [redacted]

We meet or exceed the performance levels and AQL of KPIs for IPVS as shown in C.2.2.1.4. Using the imbedded network performance tools, we collect and report current and historic information for latency, packet loss, availability, jitter, and voice quality. The Trouble Ticket system maintains and reports time-to-restore through the MetTel EIS Portal. **Exhibit 2.1.3-9** is a sample of MOS and RTT performance displayed for IPVS through the MetTel EIS Portal.

Exhibit 2.1.3-9. MOS and RTT Performance Display

2.1.3.1.8 Managed LAN Service [C.2.2.1.5]

MetTel Managed LAN service is based on the MetTel Total Care service offering and provides all the requirements to install, manage, and maintain LAN networking and hardware components and required IPVS licensing to extend the MetTel IPVS from the SDP to the terminating subscriber device (i.e., handset). MetTel Managed LAN service manages the router that terminates the access arrangement and circuit whether the solution is premise-based or network-based. All equipment provided supports Power over Ethernet (PoE) to supply the necessary power to IP phone sets or other PoE devices.

- **Survey.** A technician performs a site visit to gather information and run tests on the network interface to guarantee the best connection possible and ensure the

new circuits for IPVS are fully configured. The technician also builds a template for the Auto Attendant system if needed and identifies information such as current extension numbers, user names, and which phones need features.

- **Cabling.** If needed, cabling technicians run data cables to any locations that may not have the correct type or quantity of cable. We ensure the hardware/software solution interoperates with the Agency-provided VoIP ready cabling infrastructure which may include category 5, 5E, 6, 6A, 7, single mode, and multimode fiber. We confirm that the hardware has the proper physical interfaces to support the Managed LAN Service. All work is performed by a licensed installer. We identify any cabling limitations to the proposed solution. Any additional cabling is identified in the Task Order and performed under C.2.11 Cable and Wiring.
- **Installation.** All equipment is delivered preprogrammed for rapid implementation. Technicians install the equipment to connect the phones to our network or integrate to the existing network. They also install the phones at each desk, train users with live demonstrations, and answer any questions. [redacted]
- **Maintenance and Upgrades.** MetTel is responsible for on-going maintenance and upgrades of MetTel-owned equipment for MetTel Managed LAN service. The Agency will not incur any additional cost for device software changes or device reprogramming to meet EIS service performance levels.

[redacted]

[redacted]

- **LAN Management.** We use the MetTel EIS Portal to provide the interface and information required to support the MetTel Managed LAN service. The following are major functions provided by MetTel Managed LAN Service:
  - **Configuration Management.** MetTel provides configuration management for the life of the contracted service. The MetTel EIS Portal supports configuration management and provides real-time billing, inventory, service delivery, and repair information. We use this inventory to ensure configuration is managed to maintain hardware, software, and firmware to current tested manufacture levels.
  - **Moves, Adds, Changes, Disconnects (MACDs).** MACD requests requiring support are initiated by a Trouble Ticket through the MetTel EIS Portal. [redacted] Only authorized devices determined by the ordering Agencies operate on the Managed LAN Service.
  - **Service/Alarm Monitoring and Fault Management.** MetTel monitors, manages, and restores devices 24x7x365. We proactively notify Agency Points of Contact (PoC) within 15 minutes of an issue. The Agency staff creates a Trouble Ticket through the MetTel EIS Portal if necessary. We resolve the Trouble Ticket through standard repair procedures including trouble isolation and resolution.

- **Escalation Path for Trouble Tickets.** We work with the customer during the on-boarding process to define a Responsible, Accountable, Consult, or Inform (RACI) matrix with the Agency to ensure no issues occur during problem resolution. A RACI matrix defines roles and responsibilities of MetTel, Agency and other responsible organizations in supporting the service. Each role is identified as Responsible, Accountable, Consult, or Inform to define the type of interaction between the Agency and MetTel. The RACI document defines the escalation path for all levels of problem severity and identifies key personnel for each level of escalation as well as guidelines and timing for next steps and notifications.

Managed LAN Service does not include any wireless devices or other services (i.e., data, video, etc.) unless explicitly requested and approved by the OCO.

2.1.3.1.9 Session Initiation Protocol Trunk Service [C.2.2.1.6]

The MetTel SIP trunk service provides SIP-based network services to interconnect Customer Premises Equipment (CPE) such as PBX, SIP-enabled PBX, Key Telephone Systems (KTS), and other systems that support SIP-based IP trunk interfaces. Each business trunk represents a concurrent call or voice channel for premises equipment.

MetTel SIP Trunk service is local access neutral and can be delivered through multiple types of access, including T1/E1, DSL, and Ethernet. [redacted]

Exhibit 2.1.3-10. MetTel SIP Trunk Solutions

2.1.3.1.9.1 SIP Technical Capabilities [C.2.2.1.6.1]

MetTel SIP Trunk service provides a platform for personal and group enhanced services that can overlay features available to Hosted IPVS on the existing feature-functionality of a customer's premises equipment. SIP trunk service enables SIP users to establish and receive calls between both on-net locations and the PSTN.

[redacted]

[redacted] SIP Trunks also support off-net calling to CONUS, OCONUS and non-domestic locations and are enabled to establish and receive calls between both on-net locations and the PSTN. With multiple interconnections and geographically diverse facilities, we ensure minimal network disruptions.

2.1.3.1.9.2 SIP Features [C.2.2.1.6.2]

Our SIP trunk service provides the following required features: automatic call routing, bandwidth QoS management, trunk bursting, and phone number blocks (DID).

Automatic Call Distribution (ACD) – Provides automatic call routing by quickly routing callers to the appropriate number or agent with the correct skills and in the right priority, using a flexible set of routing policies. ACD supports functions for Call Center Services and Unified Communication Services.

Bandwidth QoS Management – Provided by MetTel at the network level to manage bandwidth and QoS allocation for voice traffic. QoS management provides effective management of IPVS services and helps allocate appropriate bandwidth to IPVS rather than require over-allocation of bandwidth.

Trunk Bursting – Allows for more trunk channels than provisioned to permit bursts of traffic, increasing the call completion rate. This enhancement is especially valuable for businesses that experience temporary surges in call activity, such as a seasonal activity or mandatory submittal date that increases calls (i.e., IRS).

Telephone Number blocks (DID) – MetTel's IPVS supports DID number blocks. [redacted]

Exhibit 2.1.3-11. MetTel SIP Trunk Architecture

2.1.4 Managed Network Services [C.2.8.1]

Agencies benefit from the vast experience and expertise of MetTel's design and engineering solutions with the MetTel Managed Network Service (MNS) solution. We apply our [redacted] to implement, manage, secure and maintain services for Agency's networks. The MetTel team's MNS provides technical, security and operational expertise and capabilities that ensure the availability, reliability and confidentiality of Agency networks. As networks become increasingly complex, our experience and expertise ensures a network environment that meets the Agency's evolving mission requirements and goals.

MetTel MNS Strengths
Small Business, Large Reach

- Recognized expertise in technical disciplines, operations and security
- Secure interactive access to all information through the MetTel EIS Portal
- Award winning customer support
- [redacted]
- MetTel EIS Portal—one-stop information source including Inventory, Billing, MACD, Procurement, and more

2.1.4.1 Compliance with Evaluation Criteria [L.29.2.1]

Our MNS solution fulfills the mandatory service requirements for MNS defined in SOW paragraph C.2.8.1. The following section presents a technical description of our offering, demonstrating our capabilities in Standards, Connectivity, Technical Capabilities, Features, Performance Metrics, and Security. **Exhibit 2.1.4-1** highlights some key strengths and benefits of our MNS solution.

Exhibit 2.1.4-1. Features and Benefits of the MetTel Solution

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• MetTel fully understands the requirements for managing the network services of Government Agencies and meeting the EIS service requirements. • The MetTel EIS Portal is the key information and communication source for MNS customers. • MNS manages the EIS services required by the Agency and is respons ble for the effective operation and deployment of the Agency network infrastructure.
Quality of Services (M.2.1(2))	• Our dedicated team implements, manages, operates, and controls Agency network environments on a secure MPLS core network and the MetTel EIS Portal provides all system information for Agencies, including SLA performance. • Our experienced team delivers MetTel MNS to be compliant, scalable, reliable, and resilient in accordance with Task Order requirements.
Service Coverage (M.2.1(3))	• [redacted]
Security (M.2.1(4))	• MetTel's network architecture ensures Agency traffic is properly identified, routed

Evaluation Criteria	Features and Benefits of MetTel's Approach
	(redirected), scanned (via DHS EINSTEIN Enclave as required), and delivered to the appropriate Agency's network. Our architecture also enables MetTel's NOC and Raytheon's SOC to identify any traffic inadvertently directed though the DHS EINSTEIN Enclave and notify DHS. Metrics (SLA KPIs) are measured in accordance with the EIS RFP. • MetTel supports the proper safeguards for handling of 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 which has recently gone through a successful A&A. • [redacted]. This preserves the confidentiality and integrity of this interconnection and ensures that agency traffic may not be inadvertently bypassed, accessed, or altered. • Our 24x7x365 SOC team is comprised of skilled and experienced analysts and engineers that are TS/SCI cleared who can be made available for "smart hands" to support DHS supplied equipment. • The SOC team will work in concert with our NOC and is responsible for device management, device tuning, security monitoring and analysis, and Digital Forensics and Incident Response (DFIR) while ensuring compliance with SLA KPIs for traffic flow through MTIPS

2.1.4.1.1 Service and Functional Description [L.29.2.1, C.2.8, C.2.8.1.1, C.2.8.1.1.1]

MetTel MNS Keys to Success
• Experienced and seasoned Project Managers to assure the Health of the Network • MetTel EIS Portal for observing the Health of the Network or understanding status of installation or repair in real-time • Experienced design and engineering team

We offer a comprehensive network management solution that comprises design and engineering, implementation, management, security and maintenance services that ensure the availability, confidentiality and reliability of increasingly complex Agency networks. We provide MNS to organizations today [redacted] that utilize our solution for telecommunications environments in a continuous state of rapid technology change with increasing bandwidth demands and complex application integration with a constant need for enhanced security, survivability, redundancy, and cost control. We recognize that Agency personnel must focus on their mission while working alongside an expert resource to ensure robust and dependable communications that provide the requisite value for the telecommunications spend. Recognizing that organizations have varying

requirements, we developed an MNS foundation that is adaptable to different requirements for size, bandwidth, and complexity. [redacted] Our MNS ensures Agency investment in services is consistent with goals by providing a single platform for consolidation of all Telecommunications Expense Management (TEM).

MetTel's MNS supports all appropriate, underlying EIS offerings to ensure seamless connectivity and complete service management. Our proactive network and security monitoring, rapid troubleshooting, and service restoration support the overall management of an Agency's network infrastructure. [redacted]

2.1.4.1.2 Standards [L.29.2.1, C.2.8.1.1.2]

MNS complies with all the appropriate standards for any underlying EIS access and transport service and the specific standards and requirements identified in an Agency Task Order as required in C.2.8.1.1.2.

2.1.4.1.3 Connectivity [L.29.2.1, C.2.8.1.1.3].

MNS works with the underlying EIS offerings of VPNS, ETS, IPVS, IPS and MTIPS as needed to ensure seamless and secure connectivity to Agency networking environments as specified in C.2.8.1.1.3.

[redacted]

2.1.4.1.4 Technical Capabilities [L.29.2.1, C.2.8.1.1.4]

We provide the required Design and Engineering services and Implementation, Management, and Maintenance services, described

below. All of which comply with security requirements set forth in the EIS RFP.

2.1.4.1.4.1 Design and Engineering Services [C.2.8.1.1.4.1]

We provide a dedicated project team to design and engineer services that fully satisfy Agency requirements. Typical tasks may include selection of hardware, firmware, and related software required by an Agency's Task Order. This includes the selection of routers, switches, firewalls, PBXs, and any other related equipment required for delivering an EIS service. Our team is dedicated to continuous improvement and current technology expertise [redacted]. We define network components, protocols, redundancy solutions, traffic filtering, and traffic prioritization requirements for QoS implementation. Additionally, we recommend bandwidth and performance levels as required to implement the network service in compliance with service KPIs.

[redacted] MetTel coordinates all installation and testing activities with the Agency to minimize impact on the current networking environment and operational mission.

2.1.4.1.4.2 Implementation, Management, and Maintenance [C.2.8.1.1.4.2]

We developed our implementation, management, and maintenance model to interact across multiple providers of service and equipment, including CLECs, Tier-1 carriers and ISPs, CPE vendors, and all major local and long distance telephone carriers. Part of this process includes defining escalation plans to predetermine the most expeditious path to elevate priorities across organizations in the event problems are not resolved through normal procedures.

Our solution implementation, management, and maintenance cover the network components, circuits, hardware, performance, and repair, as well as the administrative components of inventory control, billing, and reporting.

The MetTel EIS Portal is a key component of our Network Architecture (See **Section 1)** and is the mechanism we use to implement, maintain, and manage MNS for Agencies. The portal is powerful and secure, proprietary network-based software that provides a single, user-friendly interface for all MNS reporting requirements and real-time access to all key service information.

Agencies have secure access to current and historical information through the MetTel EIS Portal. We provide training to ensure authorized end users have full understanding of the power and information available through the MetTel EIS Portal.

Comprehensive Solutions [C.2.8.1.1.4.2 (1)]

We develop, implement, and manage comprehensive solutions constructed from components of EIS services and their enhancements. Our MNS portfolio includes the four required solutions

Exhibit 2.1.4-3. MetTel MNS Comprehensive Solutions

Solution	Goal	MetTel Approach
Access	Combination of services to meet performance metrics for availability and DR	Combine access through broadband, cable, or wireless using multiple vendors
Transport	Distribution of traffic over multiple contractor backbone networks to provide redundancy, carrier diversity, and dynamic traffic allocation	Combine multiple CLECs and ILECs services and NNIs, with Tier-1 carriers and ISPs, plus WiFi for mobility to provide diversity, redundancy, and traffic allocation needs.
Customer Premise	Agency-specific interfaces, software, or equipment	Utilize MetTel's SRE to provide the appropriate interfaces, software, and equipment required by the Task Order.
Security	Infrastructure monitoring, incident response, managed protection and implementation and maintenance requirements	Provide 24x7x365 SOC necessary to satisfy Agency requirements such as security monitoring, incident response, managed protection and implementation of firewalls, IDS/IPS, Proxy Servers, Certificate Authorities, and two factor authentication.

Supply and Manage [C.2.8.1.1.4.2 (2)]

We provision and manage all hardware, firmware, and related software required by the Agency in the Task Order. Hardware components include but are not limited to

routers, switches, encryption devices, PBXs, CSU/DSU, hubs adapters, proxy servers, firewalls, and modems (wireline or wireless). MetTel MNS supports the UNIs for all underlying EIS access and transport services implemented using MNS as required.

Customer Care [C.2.8.1.1.4.2 (3, 4, 5)]

Once an Agency issues an MNS TO, the MetTel New Client Services engages and validates engineering and assures proper understanding of management SLAs, reporting and maintenance requirements. The Agency works with Customer Care as needed via phone, email, or the MetTel EIS Portal. **Exhibit 2.1.4-4** shows the structure of the Customer Care support organization.

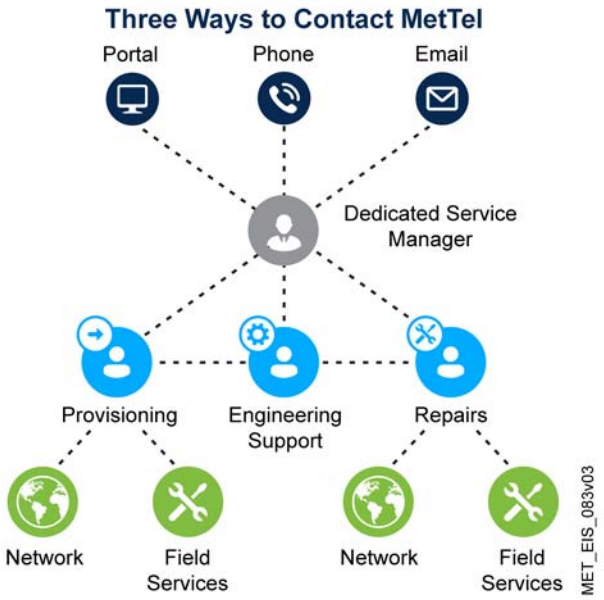


Exhibit 2.1.4-4. Customer Care

[redacted]

The MetTel EIS portal provides access to all information from Agency locations or remotely for remote management. Agencies can receive SNMP read-access data feeds which provide the Agency with managed equipment information, as required.

[redacted]

Provisioning comprises the ordering and installation of new services or sites as Agencies grow or move locations. This function includes coordinating any new circuits with the LEC or network provider as well as ordering and staging new hardware as required.

The repair function is the primary responsibility of the Network Operations Center (NOC). The NOC manages the network in real-time 24×7×365 and coordinates with the SOC to provide proactive detection of problems, responds to alerts, and provides notification of alarms, network troubles, and service interruptions. [redacted] The Centers provide remote management of equipment configurations, testing, monitoring, troubleshooting, fault/problem resolution, and maintenance.

Configuration Management [C.2.8.1.1.4.2 (6)]

The MetTel NOC also performs configuration changes consistent with Agency requirements. Changes are routine and tracked using the Trouble Ticket (TT) system. Customers can initiate a change by opening a TT in the MetTel EIS Portal, calling the NOC, or emailing the Dedicated Account Team. **Exhibit 2.1.4-5** lists typical types of routine changes that can be processed [redacted]

Exhibit 2.1.4-5. Sample Configuration Change Process

Change Request	[redacted]
Adding a protocol	
CPE Moves, Adds, Changes	
Changing addressing, filtering, and traffic prioritization schemes	
Optimizing Network Routes	
Updating equipment, software, and/or configuration (may include Firewalls and VPN devices)	
Upgrading or downgrading bandwidth	
Implementing configuration changes for all agency-specific devices	
Maintaining a configuration database for all agency-specified devices	
Auditing government router configurations	

Network Operations Center Support [C.2.8.1.1.4.2 (7, 8, 9, 10, 11, 12)]

As the organization responsible for O&M of the Agency's MNS, the MetTel NOC provides Agency support for many functions and services, including implementation and

design. **Exhibit 2.1.4-6** shows a representative table of support provided by the Customer Care Center through the NOC as well as our management and maintenance processes.

Exhibit 2.1.4-6. Customer Care Services for MNS Agencies

Service	MetTel Approach
IP address management	Supply registered IP addresses to the Agency as required and in accordance with ARIN IP address allocation requirements. Assist with transitioning non-registered private IP addresses (RFC 1918) to public addresses for routing purposes
Monitor and control access to equipment	Monitor and control access to equipment under MetTel control using appropriate authentication and role-based user permissions as directed by the Agency. [redacted] Enforce two-factor authentication for all remote network access using TACACS with tokens, RADIUS, or VPN (based on SSL/TLS or IPSEC) with individual certificates.
Off-site equipment configuration backup	Regularly perform off-site equipment configuration backups to a data center-based backup repository. Perform backups on a regular basis and whenever a change to the device configuration is made to ensure fallback is able to restore the previous configuration. Log all backups and provide the Agency access to backup logs as necessary
Hardware and software upgrades	Customer Care Center implements necessary hardware and software upgrades, updates, patch deployment, and bug fixes as soon as they become available and are tested. Coordinate with the Agency to test new releases and implement upgrades. Test new releases that address or resolve security issues to ensure compatibility with the Agency environment, minimize service disruptions, and maintain equipment functionality.
Preventive and corrective maintenance	Provide preventive and corrective maintenance as defined in the Task Order for Agency-specific devices.
Proactive problem detection	Help Desk working in conjunction with the NOC and SOC proactively detects problems, responds to alerts, and promptly reports situations that adversely affect throughput to the impacted Agency via email or phone or as directed by the Agency in the Task Order. • Monitoring – (a) Monitor Agency-specific network availability and QoS, including circuit availability, latency, jitter, packet delivery, and packet loss; (b) access circuits availability and QoS; (c) edge router availability, and performance; (d) transport service availability at the government's network equipment; (e) agency-specific network performance from government network equipment to government network equipment; (f) transport service performance up to the government network equipment; (g) transport service performance from government network equipment to government network equipment. (h) Provide, monitor, and manage circuits for out-of-band government network equipment. • Open/close TTs – (i) Open TTs in the Agency TT system; (j) In MetTel trouble management system, and partner provider trouble management systems through ebonding. • Troubleshooting – (k) Troubleshoot faults for access and transport services; (l) Government network equipment; (m) Agency-specific network faults and coordinate fault resolution and repair; (n) Notify agency-specific network users of faults and maintenance via agency alerts. • NOC Support – (o)Provide a NOC Help Desk to answer phones and respond to email and

Service	MetTel Approach
	MetTel EIS Portal TT requests. (p) The NOC provides Tier-1, Tier-2, and Tier-3 support to the Agency NOC for MetTel access and transport services; (q) Support to agency NOC for components of the agency network that are managed by MetTel.
Rules of engagement	Customer Care predefines a RACI matrix with the Agency to ensure no issues during problem resolution. A RACI matrix defines roles and responsibilities of the Agency and other responsible organizations in supporting the service. Each role is identified as Responsible, Accountable, Consult, or Inform to define the type of interaction between the customer and MetTel.

MetTel EIS Portal – Information Source for MNS [C.2.8.1.1.4.2 (13, 14, 15)]

MetTel provides users access to the MetTel EIS Portal with role-based user permissions as determined by the Agency. The portal provides users with a single, user-friendly source of information for all real-time and historical information about the MNS. [redacted]

[redacted]

Agency administrators add users to job-related roles and edit and modify user permissions to manage user access to Agency information as needed.

Installation Schedule [C.2.8.1.1.4.2 (13 a)]

The MetTel EIS Portal provides authorized Agency personnel with near-real-time access to the installation schedule through the NCS Tracker. The NCS Tracker provides detailed activity schedules for equipment delivery and installation, access and transport circuits including FOC dates when available, ports, and permanent virtual circuits (PVCs) as applicable to the solution. The installation schedule provides the Agency the ability to track the provisioning process through completion at any time through the MetTel EIS Portal.

Network Statistics and Performance Management [C.2.8.1.1.4.2 (13 b)]

We provide a rich set of performance information displays with real or near-real time access. Through the MetTel EIS Portal, Agency users can access network statistics and performance information including MPLS link monitoring, QoS performance, traffic monitoring, and security logs. **Exhibit 2.1.4-8** shows an example of the types of performance screens available to Agency users.

Exhibit 2.1.4-8. MetTel EIS Portal Network Performance Examples

As shown in **Exhibit 2.1.4-8**, we provide authorized users secure access to current and historical performance information through the MetTel EIS Portal. Depending on Task Order requirements, the MetTel EIS Portal provides graphic and tabular information about services provided to the Agency. This information includes but is not limited to network performance information for the data types defined in **Exhibit 2.1.4-9.**

Exhibit 2.1.4-9. MetTel EIS Portal Network Performance Information

Inventory Management [C.2.8.1.1.4.2 (14)]

Our full-featured inventory system ensures Agency users have real-time status of inventory. Authorized users can search for lines, circuits, hardware (MetTel-provided or GFP), or accounts using multiple criteria through the inventory management system. The SOC has inventory information permissions to aid in any incident response, hunting and vulnerability scanning. **Exhibit 2.1.4-10** depicts the MetTel EIS Portal Equipment Inventory Information screen.

Exhibit 2.1.4-10. MetTel Portal Equipment Inventory Information

Trouble Ticket (TT) Management [C.2.8.1.1.4.2 (13 c, d)]

The MetTel EIS Portal is the secure window to the MetTel TT Management System.

Users submit TTs to request security logs, network maps, and performance report resolution. **Exhibit 2.1.4-11** illustrates a sample EIS Portal Trouble Ticketing Management screen.

Exhibit 2.1.4-11. MetTel Trouble Ticket Management

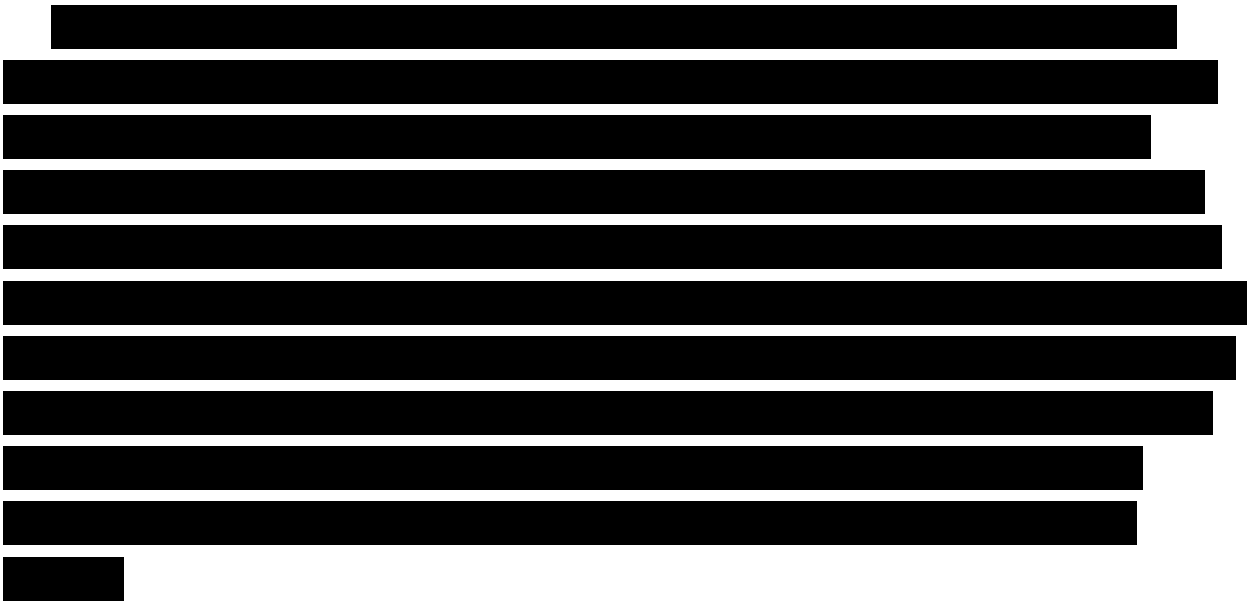
2.1.4.1.5 Features [L.29.2.1, C.2.8.1.2]

MetTel provides the following services:

1. **GFP and SRE Maintenance**. Maintain and repair SRE and GFP as required.
2. **Agency-specific NOC and SOC**. Customer-specific help desk services and shared and dedicated NOCs and SOCs to meet Agency requirements specified in a Task Order. Utilizing the strengths of the NOC's ability to understand the network baseline, the SOC will investigate anomalous traffic as identified by the data flowing into the NOC from the network and SRE. Our SOC leverages the MetTel Trouble Ticket Management (TTM) to search, source and correlate data for ingestion into the Advanced Threat Intelligence Platform (ATIP). ATIP in turn supports 24x7x365 security monitoring, it aids in advanced hunting and provides data for the incident response lifecycle.

3. Network Testing. Support Agency-specific development services that address the Agency's potential need to test equipment, software, and applications on the MetTel network prior to purchase and deployment. These testing efforts are managed through the Trouble Ticketing Management system and cover voice, data, and video technologies that may or may not be over an IP VPN. Testing is performed at the discretion of the Agency and structured in collaboration with MetTel.

4. Traffic Aggregation Service (DHS Only). MetTel service offerings under EIS (e.g., VPNS, Ethernet Transport, IPS, MTIPS, and IPSS) that transport Internet, Extranet, and Inter-Agency traffic identifies and routes the applicable government traffic through a secure DHS EINSTEIN Enclave for processing by the latest generation of DHS EINSTEIN capabilities. MetTel has identified multiple existing locations in Northern, Virginia that are ANSI/TIA-942 and ICD 705 certified facilities that can serve as DHS EINSTEIN Enclaves. The physical technology implementing the DHS EINSTEIN Enclave will be hosted in secure environments appropriate for the sensitivity of the specific DHS EINSTEIN Enclave. Network connectivity including secured data communication, if required is provided between the DHS EINSTEIN Enclave hosted equipment and DHS data centers.



MetTel assumes all responsibility for the installation, configuration, maintenance and repair of the MetTel infrastructure that implements the traffic aggregation capability and the communication services that support interconnection of the DHS EINSTEIN Enclave

equipment to the MetTel infrastructure. This includes the engineering services to accomplish the integration of the DHS EINSTEIN Enclave sensor equipment, data centers, and data communications to the MetTel EIS infrastructure.

MetTel personnel are prepared to assist with the installation, configuration, maintenance and repair of the DHS EINSTEIN Enclave sensor systems. Our personnel performing these functions possess the training, experience and required security clearance / suitability to provide “Smart-Hands” service to the DHS EINSTEIN Enclave supplied equipment.

2.1.4.1.6 Interfaces [L.29.2.1, C.2.8.1.3]

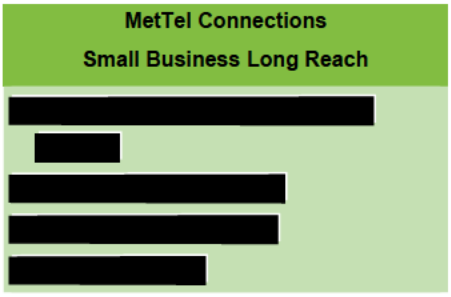
MNS supports the UNIs for all underlying EIS access and transport services.

2.1.4.1.7 Performance Metrics [L.29.2.1, C.2.8.1.4]

We support the performance metrics for MNS as specified in a Task Order. The MetTel EIS Portal provides the interface for the Agency to view and interact with MNS personnel on service issues.

We meet or exceed the values of the KPIs for MNS and all underlying EIS network services we manage. [redacted]

2.1.5 Access Arrangements [C.2.9, F.2.1 (28)]



Access Arrangement (AA) is a key part of the MetTel standard delivery model, and we stand ready to provide the best choice in AA to meet the diverse needs of Agency users. We built our business as a true telecommunications integrator providing the best solution with the best price. We have multiple AA providers in most CBSA and use this competitive edge to offer the most cost-effective, reliable solution for the Government. We have wholesale partnerships with most of the Local Exchange Carriers (LECs), Tier-1 carriers and ISPs, and cable and wireless providers. Through these partnerships, we provide the right technology complete with customized access, required diversity, and path avoidance. With this approach, we have eliminated the constraints of a single provider, single access provider, or single hardware vendor. We have the freedom to select the most cost-effective, best technological access solution based on the location, bandwidth, and survivability requirements.

AAs provide connections between the Agency SDP and the network POP. We provide customized AAs that provide enhanced diversity and survivability. Several examples of customized AAs follow.

2.1.5.1 Compliance with Evaluation Criteria [L.29.2.1]

The MetTel AAs fulfill the mandatory service requirements contained in C.2.9. This section presents a technical description of our offering, demonstrating our capabilities in Standards, Connectivity, Technical Capabilities, Features, Performance Metrics, and Security. **Exhibit 2.1.5-1** highlights some key strengths and benefits of our AA solution in relation to RFP Section M.2.1 evaluation criteria.

Exhibit 2.1.5-1. Features and Benefits of MetTel Access Arrangements

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• 20 years of experience providing AAs to industry and Government • Architecture that allows MetTel to offer the largest selection of access types and speeds from LECs, Tier-1 providers, and cable and wireless providers • Reach to more locations than any single provider • [redacted]
Quality of Services (M.2.1(2))	• AAs support the network or application service that rides over the network and the KPIs of those services with compliant connections

Evaluation Criteria	Features and Benefits of MetTel's Approach
	• 24x7x365 live customer support [redacted] • Infrastructure that provides high availability and allows MetTel to meet required TTR intervals
Service Coverage (M.2.1(3))	• Larger footprint than any single provider, allowing MetTel to provide the right AA at the most competitive price in any CBSA or location • [redacted]
Security (M.2.1(4))	• Strong partnership with access providers that comply with Agency security requirements • Onsite technicians verified as U.S. citizens when necessary • Telco facilities that provide access controls to protect the local access providers' end of the AA

2.1.5.1.1 Service and Functional Description [L.29.2.1, C.2.9.1, C.2.9.1.1]

Access management is a key part of the MetTel standard delivery model and we are in a unique position to provide Agencies the best choice in AA. [redacted]. We have wholesale partnerships with most of the LECs, Tier-1 network providers, and cable and wireless providers. Through these partnerships, we provide the right technology to the customer complete with customized access and required diversity and path avoidance.

AAs provide connections between the Agency SDP and the network POP. We provide customized AAs that provide enhanced diversity and survivability. The following are examples of diverse AAs.

Physically disparate, diverse paths from the SDP to two diverse contractors' POPs

This configuration comprises two options: 1) the paths are diverse to two different POPs in the MetTel network, or 2) the second POP is in a second network provider's network and then connected to the MetTel network through the standard NNI with that network provider. The first solution is typically used for locations threatened by disruption due to natural disasters. For example, this scenario has been used effectively to provide redundancy in New Orleans, LA by providing access to two POPs in the MetTel network: [redacted] **Exhibit 2.1.5-2** depicts this customized AA.

Exhibit 2.1.5-2. Diverse Paths from the SDP to Two Diverse Contractors' POPs

A variation to this diversity allows the second connection to be to an alternate provider network and connect to one of its POPs. This AA provides two diverse paths to disparate network providers: MetTel and an alternate provider network. **Exhibit 2.1.5-3** depicts this type of AA. The site in [redacted] would have a path to the MetTel NYC POP and a second to an alternate provider's network [redacted] with connectivity not running across any cable, facilities, or common fiber.

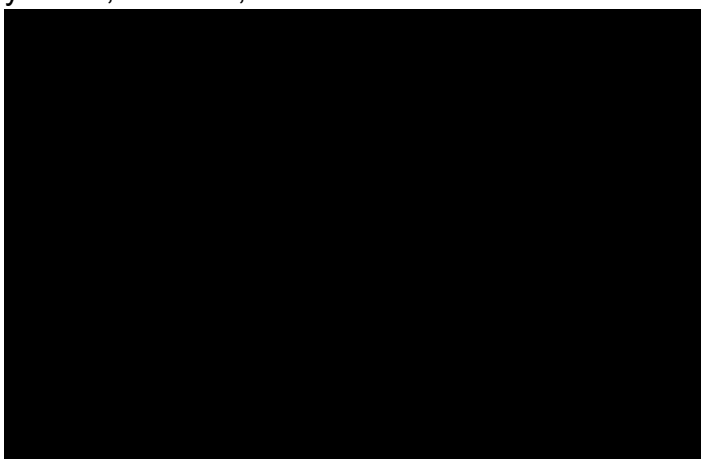


Exhibit 2.1.5-3. Diverse Paths from the SDP to Two Providers' POPs

Physically disparate, diverse paths from the SDP to the MetTel POP

Providing path diversity to the same POP requires designing the AA to avoid passing through the same telecommunications facility or over the same cable or fiber runs.

Minimum separation is 30 feet between the diverse routes and buildings where an SDP and its associated network connecting points are housed. Vertical separation is at least 2 feet with cables separately encased in steel or concrete for cable crossovers. This is achieved by building the two circuits using two disparate and diverse Serving Wire Centers (SWCs) and ensuring that the paths do not have any common elements.

Switching between the two routes is achieved by setting up BGP weighting so the primary path is used when available and a second path is used as an alternate. This can also be extended to use two different technologies' AA (e.g., one AA could be Ethernet and the other TDM DS-3). **Exhibit 2.1.5-4** shows an example of this type of configuration.

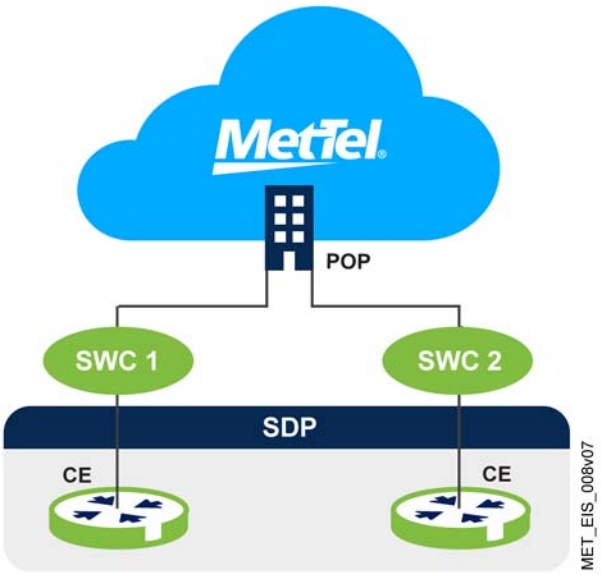


Exhibit 2.1.5-4. Physically Diverse Paths to a Single MetTel POP

Redundant paths from an SDP to the MetTel POP

This configuration provides redundant connections from the SDP to the MetTel POP. Both circuits can be used to pass traffic, or one could be configured using BGP as a hot stand-by for the other. Terminating each circuit in a different router provides protection against a single router or circuit failure interrupting service. The circuits terminate in different PE routers at the MetTel POP. **Exhibit 2.1.5-5** shows redundant paths between the SDP and the MetTel POP.

Exhibit 2.1.5-5. Redundant Paths from an SDP to the MetTel POP

Redundancy through Ring Architecture

An additional form of redundancy is achieved by using SONET ring technology for the AA for one circuit and TDM technology for the second. In **Exhibit 2.1.5-6**, both circuits go to the same MetTel POP—the primary being a SONET ring with its self-healing capabilities and the redundant circuit being a TDM or other technology. In this configuration, both can be active or one can be active and the second a failover circuit.

Exhibit 2.1.5-6. Redundant and Disparate Paths from an SDP to the MetTel POP

Special Construction

We use all of our wholesale partnerships with local access providers to ensure all other options have been considered prior to initiating a special construction process necessary for services or facilities related to the delivery of an AA. Two general cases may require MetTel to initiate a special construction engagement:

1. If AA does not exist or does not have sufficient capacity and we must provide special construction by implementing, rearranging, or relocating a physical plant solely to comply with the Government's AA request.
2. If we require special construction to implement a different route. This can be from Government premise to PCL, PCL to an alternate contractor's POP, or some other route than we would otherwise use to provide the AA.

When special construction is required, we survey potential operational locations to collect and validate floor plans, physical measurements, building power capacity, equipment space and location, and external ingress/egress factors that impact the cost of special construction. We complete the physical inspection of the locations and deliver site survey reports in accordance with EIS RFP Section J.10 Special Construction Template for Site Survey Report.

2.1.5.1.2 Standards [L.29.2.1, C.2.9.1.2]

AAs comply with all standards defined in RFP Section C.2.9.1.2 and listed in **Exhibit 2.1.5-7** with the appropriate AA from RFP Section C.2.9.1.4.

2.1.5.1.3 Connectivity [L.29.2.1, C.2.9.1.3]

AAs are the connections between the SDP and the POP and interoperate with Agency-specified locations and equipment and the MetTel POP network.

2.1.5.1.4 Technical Capabilities [L.29.2.1, C.2.9.1.4]

We built our network architecture on standards-based AAs and comply with all the standards listed in EIS RFP C.2.9.1.4 and defined in Exhibit 2.1.5-7. AAs provide integrated access of differentiated services and are transparent to any protocol. Exhibit 2.1.5-7 lists the MetTel-supported AAs and the standards associated with each.

Exhibit 2.1.5-7. Supported Access Arrangements and Standards

Access Arrangement	Channels and Line Rate	Un-channelized or Concatenated Payload or Increments	Notes and Standards
T-1	24 – DS0 (56/64 kb/s) 1.544 Mbps	1.536 Mbps	1. ANSI T1.102/107/403/503/510 for T1
ISDN PRI	23 – DS0 (56/64 kb/s) ISDN PRI (23B+D) 1.544 Mbps	1.544 Mbps	2. ANSI T1.607/610 for ISDN PRI
ISDN BRI	2 – DS0 (56/54 Kbps) ISDN BRI (2B+D) 144 Kbps		2. ANSI T1.607/610 for ISDN PRI
T-3	28 – DS1 (1.536 Mbps) 44.736 Mbps	43,008 Mbps	3. Telcordia PUB GR-499-CORE for T3
E-1 (Non-domestic)	30 – DS0 (56/64 kb/s) 2.048 Mbps	1.92 Mbps	6. ITU-TSS G.702 and related recommendations for E1 and E3
E-3 (Non-domestic)	16 – E1 (1.92 Mbps) 34.368 Mbps	30.72 Mbps	6. ITU-TSS G.702 and related recommendations for E1 and E3
SONET OC-3	3 – OC-1 (49.536 Mbps) 622,080 Mbps	148.608 Mbps	OC-3c is concatenated 4. ANSI T1.105 and 106 for SONET 5. Telcordia PUB GR-253-CORE for SONET
SONET OC-12	4 – OC-3 (148.608 Mbps) 622.080 Mbps	594.432 Mbps	OC-12c is concatenated 4. ANSI T1.105 and 106 for SONET 5. Telcordia PUB GR-253-CORE for SONET
SONET OC-48	4 – OC-12 (594.432 Mbps) 2.488 Gbps	2.377728 Gbps	OC-48c is concatenated 4. ANSI T1.105 and 106 for SONET 5. Telcordia PUB GR-253-CORE for SONET
SONET OC-192	4 – OC-48 (2.488 Gbps) 10 Gbps	9.510912 Gbps	OC-192c is concatenated 4. ANSI T1.105 and 106 for SONET 5. Telcordia PUB GR-253-CORE for SONET
[redacted]	[redacted]	[redacted]	[redacted]
Analog Line	2 Wire 4 KHz	N/A	2 wire analog lines and trunks without access integration for voice
DS0	56 Kbps and 64 Kbps	N/A	
[redacted]	[redacted]		[redacted]
Optical Wavelength	a) 1 Gbps		Bi-directional wavelengths (WDM)

Access Arrangement	Channels and Line Rate	Un-channelized or Concatenated Payload or Increments	Notes and Standards
	b) 2.5 Gbps c) 10 Gbps d) 40 Gbps		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 Not offered by MetTel.
[redacted]	[redacted]	[redacted]	[redacted]
DSL 1. ADSL 2. SDSL 3. ISDN DSL (Optional)	 Upstream 16 to 768 Kbps Downstream 1.5 to 8 Mbps Up to and including 1.5 Mbps Up and down 144 Kbps	 Asymmetric Up to 50 Mbps (Optional) Symmetric Up to 2.3 Mbps (Optional) (Not offered)	11. 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) Not offered by MetTel.
Ethernet (Optional) (Optional)	1 Mbps to 10 Mbps 10 Mbps to 100 Mbps 100 Mbps to 1 Gbps 2 Gbps to 10 Gbps 10 Gbps to 100 Gbps	1 Mbps increments 10 Mbps increments 100 Mbps increments 1 Gbps increments 10 Gbps increments	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 ba) Not offered by MetTel.
Cable High-Speed (OPTIONAL)	256 Kbps to 5 Mbps 256 Kbps to 10 Mbps 256 Kbps to 150 Mbps		Standard DOCSIS 1.0 Standard DOCSIS 1.1 Standard DOCSIS 3.0
[redacted]			[redacted]
Wireless a) Cellular Service b) Line of Sight	 100 Mbps (downstream) 50 Mbps (upstream) DS1 NxDS1 (where N=2 to 27 DS3 E1 NxE1 (where N=2 to 15) E3 SONET OC-3 1 Gbps, 5 Gbps and 10 Gbps		 4G Long-term Evolution (LTE) Using licensed frequencies and technology specified in the Task Order. (Non-domestic) (Non-domestic) (Non-domestic)

2.1.5.1.5 Access Diversity and Avoidance [L.29.2.1, C.2.9.2]

Access Route or Path Diversity

We provide access route and path diversity on at least two physically separated routes for access diversity. The following options for access route and path diversity are available:

1. Between an SDP and its associated connecting network's PCL or POP. Exhibit 2.1.5-5 and Exhibit 2.1.5-6 show this option.
2. Between an SDP and at least two connecting network PCL/POPs. Exhibit 2.1.5-2 shows this configuration.
3. Access from the same or different access providers (e.g., LEC or CLEC) for two separate routes, using any mix of AAs. Exhibits 2.1.5-3 and 2.1.5-4 show this configuration.

Diverse routes meet the following requirements:

1. No sharing of common telecommunications facilities, offices, or common building entrance.
2. Minimum separation of 30 feet maintained for all diverse routes between premises/buildings where an SDP and its associated network connecting point are housed.
3. Minimum vertical separation of 2 feet, with cables encased (separately) in steel or concrete for cable crossovers.

We provide the routing protocol (i.e., BGP etc.) for automatic switching of transmission in real-time, negotiated on an individual basis at the time of Task Order. Automatic switching occurs in the following two cases:

1. From the primary access route to one or more diverse access routes, including satellite connections.
2. From the diverse access route to the primary access route once the primary has resumed an operational status.

Access Route or Path Avoidance

We allow the Agency to identify and define a geographic location or route to avoid between an SDP and its associated connecting network point (PCI/POP). This requirement is defined in the Agency Task Order.

Control, Representation, and Management of Diverse, Disparate, and Avoidance Routes

We provide overall management and control of diverse path and path avoidance designs and implementations. During the design phase of diverse, disparate and avoidance routes, we create graphical representation of access circuit routes to show where diversity has been implemented. We provide these diagrams to the OCO with the as-built implementation of access diversity or avoidance within 30 calendar days of implementation of circuit routes and again anytime a change is made.

We collaborate with local access providers prior to any proposed reconfiguration or re-grooming that would impact routes previously configured for access diversity or avoidance. We provide written notification and revised Physical Concentration Locations (PCLs) for OCO approval in accordance with the requirements of the Task Order.

Agencies can specify in a Task Order that a route or path must avoid passing through or near an SDP and its associated connecting network points (i.e., Serving Wire Centers). This is a special case of diversity and disparity that requires the same detail definition and management. We create graphical representation of the circuit layout showing where avoidance has been implemented. We provide these diagrams to the OCO within 30 calendar days of the implementation of avoidance and again anytime a change is made. Prior to any reconfiguration of routes previously configured for avoidance, we provide written notification and revised PCLs to the OCO for review and approval in accordance with the requirements of the Task Order.

All diverse, disparate, or avoidance circuits are identified in our management platform. Interactions with LECs and Tier-1 providers also tag circuits with these requirements and are reviewed with the providing entity prior to any change. Additionally, we meet with the AA providers at least quarterly to review all circuits tagged with diversity, disparate, avoidance, or other special requirements such as TSP priorities. Agencies are notified within 5 business days of any proposed changes or modifications to diverse, disparate, or avoidance tagged circuits.

2.1.5.1.6 Interfaces [L.29.2.1, C.2.9.3]

Exhibit 2.1.5-8 defines the SRE in the SRE Catalogue for each of the UNI Types required by EIS RFP Section C.2.9.3. The SRE interfaces are in the Notes column of the SRE Catalogue.

Exhibit 2.1.5-8. SRE Interfaces for AA UNIs

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type	SRE Configuration Item
1	ITU-TSS V.35	Up to 1.92 Mbps	Transparent	AA-1
2	EIA RS-449	Up to 1.92 Mbps	Transparent	AA-2
3	EIA RS-232	Up to 19.2 Kbps	Transparent	AA-3
4	EIA RS-530	Up to 1.92 Mbps	Transparent	AA-4
5	T1 (with ESF) (Std: Telcordia SR-TSV-002275; ANSI T1.403)	Up to 1.536 Mbps	Transparent IP (v4/v6)	AA-5
6	ISDN PRI (23B+D and 24B+0D) (Std: ANSI T1.607/610)	Up to 1.472 Mbps	Transparent	AA-6
7	T3 (Std: Telcordia GR-400-CORE)	Up to 43.008 Mbps	Transparent	AA-7
8	E1 (Std: ITU-TSS)	Up to 1.92 Mbps G.702) (Non- domestic)	Transparent	AA-8
9	E3 (Std: ITU-TSS G.702) (Non-domestic)	Up to 30.72 Mbps	Transparent	AA-9
10	SONET OC-3 (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent	AA-10
11	SONET OC-3c (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent	AA-11
12	SONET OC-12 (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent	AA-12
13	SONET OC-12c (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent	AA-13
14	SONET OC-48 (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent	AA-14
15	SONET OC-48c (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent	AA-15
16	SONET OC-192 (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent	AA-16
17	SONET OC-192c (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent	AA-17
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type	SRE Configuration Item
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
20	10 Base-T/TX/FX (Std: IEEE 802.3)	Link bandwidth: Up to 10 Mbps	IP (v4/v6) IEEE 802.3 Ethernet MAC (for bridging)	AA-20
21	100 Base-TX/FX (Std: IEEE 802.3)	Link bandwidth: Up to 100 Mbps	IP (v4/v6) IEEE 802.3 Ethernet MAC (for bridging)	AA-21
22	1000 Base-T/L/LX/B/BX/PX (Std: IEEE 802.3)	Link bandwidth: Up to 1 Gbps	IP (v4/v6) IEEE 802.3 Ethernet MAC (for bridging)	AA-22
23	10 Gbps (Std: IEEE 802.3)	Link bandwidth: Up to 10 Gbps	IP (v4/v6) IEEE 802.3 Ethernet MAC (for bridging)	AA-23
24	Reserved			
25	ISDN BRI (2B+D) (Multirate) [Standard: ANSI T1.607 and 610]	144 Kbps	ITU-TSS Q.931 IP (v4/v6)	AA-25
26	3G / 4G / 4G LTE (Cellular Service)	Up to current standard	ITU 3GPP TR25.913 IP (v4/v6)	AA-26

2.1.6 Internet Protocol Service [C.2.1.7]

MetTel Internet as a Commodity
• Access and bandwidth to meet Agency growing needs to serve customers • Global reach [redacted] • Award winning customer support (CSO)

MetTel Internet Protocol Service (IPS) provides support for the full range of connection requirements for Agencies to the Internet. MetTel and our premier Internet providers have extensive reach, connection options, and interface types to meet Agency requirements for connections using TCP/IP protocol suit.

2.1.6.1 Compliance with Evaluation Criteria [L.29.2.1]

The MetTel IPS solution fulfills the mandatory service requirements for IPS defined in SOW paragraph C.2.1.7. The following section presents a technical description of our offering, demonstrating our capabilities in the following areas: Standards, Connectivity, Technical Capabilities, Features, Interfaces, Performance Metrics, and Security. **Exhibit 2.1.6-1** highlights some key strengths and benefits of our IPS solution in relation to RFP Section M.2.1 evaluation criteria.

Exhibit 2.1.6-1. Features and Benefits of Approach to IPS

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• 20 years of experience providing IPS to industry and Government • IPS provides a single solution for Agency-level, reliable connections that complement existing services, such as security, Virtual Private Networks (VPNs), Voice over Internet-Protocol (IPVS), private networking, and Managed Services (MNS). • IPS supports both IPv4 and IPv6 • [redacted] • IPS provides strong KPIs and performance options to support mission-critical communications
Quality of Services (M.2.1(2))	[redacted] Full compliance with all SOW performance metrics (see Section 2.1.7.4) [redacted] • 24x7 live customer support and proactive service monitoring • IPS provides high availability from rigorously engineered backbone networks designed for high performance
Service Coverage (M.2.1(3))	• Global and scalable enterprise-level IP network connectivity that offers multiple, full-duplex bandwidth options [redacted] • Support for hybrid networking and dual-stack (IPv4 and IPv6) options within the U.S., EMEA, and Asia-Pacific regions. • [redacted]
Security (M.2.1(4))	• MetTel's network architecture ensures that Agency traffic is properly identified, routed (redirected), scanned and monitored (via DHS EINSTEIN Enclaves), and delivered to the

Evaluation Criteria	Features and Benefits of MetTel's Approach
	appropriate agency's network. It also enables MetTel and the Raytheon SOC to identify any traffic that has been inadvertently directed through the DHS EINSTEIN Enclave and notify DHS. Additionally, metrics (SLA KPI's) shall be measured in accordance with the EIS RFP. • MetTel supports the proper safeguards for handling of traffic should failures occur with the DHS GFP. Additionally, all DHS EINSTEIN Enclaves will be housed within a planned ANSI/TIA-942 and ICD 705 certified facility in Northern Virginia. • IPS supports BGP sessions protected with MD5 signature option as defined in NIST SP 800-54.

2.1.6.1.1 Service and Functional Description [L.29.2.1, C.2.1.7.1, C.2.1.7.1.1]

Internet users expect Internet access to be consistently available with robust performance. MetTel IPS provides the integration of the top Internet networks with the right access to provide the Internet to Agency users and customers. IPS supports a wide range of connectivity options that enable the Government user to access the Internet, Government-wide Intranets, and Extranets. IPS uses the TCP/IP (IPv4 and IPv6) protocol suite to transport IP packets and interconnect GFP and SRE with other Government networks and the public Internet Service Provider (ISP) networks.

MetTel meets all the requirements of Section C.2.1.7, IPS. MetTel combines the strength of global wholesale partnerships with the flexibility of the best local access provider to meet the customer's Internet connectivity requirements. Our IPS is a mature offering with proven technology and capabilities that ensure low risk in terms of outages, Denial of Service (DoS) attacks, and performance on an IPS link. Customer support provides timely and proactive operation to address service issues that can severely affect day-to-day operations. [redacted]

IPS is supported by the appropriate Service Related Equipment (SREs) with the appropriate interfaces as required by service/speed type to deliver maximum efficiency and cost effectiveness. IPS has multiple SREs options available, based on service type, speed, etc. [redacted]

IPS provides flexible access methods that connect and traverse the MetTel IPS

network and provide Internet, Intranet, and Extranet services. For Internet access, Agencies can connect directly or indirectly using any of the access methods listed above. Service delivery of the access includes installation, configuration, maintenance, support, project management, and testing. Additionally, MetTel has various wholesale providers for off-net access to offer greater availability with extended access footprint consisting of DSL, Cable, Wireless, and Satellite. [redacted] MetTel selects the best provider based on facilities (i.e., lit buildings), ability to meet the service requirement, cost, and best overall value. Strategic partner selection enhances the coverage needed to meet and exceed the mandatory CBSA requirements of the EIS RFP. **Exhibit 2.1.6-2** shows the reach achieved by MetTel through our preferred partners for IPS.

Exhibit 2.1.6-2. Preferred Partner Reach for IPS

MetTel and our wholesale partners' IPS offering meets all the requirements defined in the EIS RFP Section C.2.1.6. Our IPS solution features reliable, technically advanced IP capabilities and feature sets. MetTel wholesale partners are established leaders in IP network technology and provide a global Internet backbone that spans six continents and more than 140 countries.

2.1.6.1.2 Standards [L.29.2.1, C.2.1.7.1.2]

MetTel as an integrator of networks relies on standards to ensure proper and compliant service is delivered to MetTel customers. We comply with the standards listed in EIS RFP Section C.2.1.7.1.2 and all new versions, amendments, and modifications of these standards.

2.1.6.1.3 Connectivity [L.29.2.1, C.2.1.7.1.3]

MetTel IPS connects Government locations including mobile and remote users and SDP devices such as customer routers, switches, firewalls, and SRE to the internet. The Internet's wide use as a preferred communication media means it must be accessible from a wide range of equipment such as tablets, notebook PCs, PDAs, and mobile phones. The appropriate combinations of EIS services to the internet provide connections through IPS. MetTel IPS connects Government locations to other networks including those of other EIS contractors. MetTel IPS provides seamless connectivity to the largest set of ISPs to provide universal connectivity to all the required components.

2.1.6.1.4 Technical Capabilities [L.29.2.1, C.2.1.7.1.4]

MetTel IPS provides all the technical capabilities required by the EIS RFP Section C.2.1.7.1.4. **Exhibit 2.1.6-3** provides the MetTel response to these technical capabilities.

Exhibit 2.1.6-3. MetTel IPS Capabilities

Capability	MetTel Response
1. Section C.1.8.8 Security	MetTel's network architecture ensures that Agency traffic is properly identified, routed (redirected), scanned and monitored (via EINSTEIN enclaves), and delivered to the appropriate agencies network. It also enables MetTel to identify any traffic that has been inadvertently directed through the EINSTEIN enclave and notify DHS. Additionally, metrics (SLA KPI's) shall be measured in accordance with the EIS RFP.
2. IPS Ports	MetTel provides full throughput at peak data rates specified by the Agency in the Task Order.
3. Appropriate access service	[redacted]
4. Peering, IP Addresses, DNS	a) MetTel provides public peering arrangements to the Internet. The combination of all our wholesale ISP partners has the largest public peering capacity in the market today. b) MetTel provides direct/private peering to exchange Internet traffic over multiple dedicated interconnects; the cost is shared between peers. Private interconnections enable MetTel and peers to determine the precise speed, location, and terms through which the two carriers meet. Direct peering also provides greater control over the quality of service at each interconnection point, because ISP is not relying on a third party to maintain equipment.

Capability	MetTel Response
	c) MetTel supports Government-assigned and InterNIC-registered IP addresses and domain names. IP address allocation is in conformance with InterNIC requirements and may require the submission of an IP address Justification Form to comply with IP address allocation policies. d) MetTel provides Primary and Secondary Domain Name Service (DNS) to provide authoritative name server for Agencies in accordance with NIST SP 800-81-2 recommendations for Secure DNS deployments.
5. Border Gateway Protocol (BGP)	MetTel provides and supports the BGP (BGPv4) for EIS customers with registered Autonomous System (AS) numbers.
6. Authenticated Protocols	MetTel validates routing protocol information using authenticated protocols. BGP sessions are configured in accordance with, but not limited to, the NIST SP 800-54 recommendation that BGP sessions be protected with the MD5 signature option.

2.1.6.1.5 Features [L.29.2.1, C.2.1.7.2]

MetTel accommodates and optimizes an Agency's applications to enable the network to accurately and consistently allow for traffic prioritization and cost-efficiencies. [redacted] Based on the traffic priorities set by the Agency, the various traffic flows are provided a portion of bandwidth that favors higher priority traffic over lower priority traffic during times of congestion.

Exhibit 2.1.6-4 defines the IPS QoS traffic priority classes.

Exhibit 2.1.6-4. IPS QoS Traffic Priority Classes

Class of Service	Name of Priority Class	Characteristics
Premium	Expedited Forwarding (EF)	• Highest forwarding priority • Low latency, low jitter • Strict forwarding priority • Can access 100% of port bandwidth
Enhanced	[redacted]	• Next highest forwarding priority • Class-based weighted fair queuing [redacted] • Can access unused bandwidth not assigned to EF
Standard	Best Effort (BE)	• Lowest priority • Class-based weighted fair queuing • Can access unused bandwidth not assigned to EF

2.1.6.1.6 Interfaces [L.29.2.1, C.2.1.7.3]

Exhibit 2.1.6-5 defines all the interfaces supported by MetTel. Listed are SRE

components that satisfy the interface, bandwidth, and connectivity options. SRE pricing is in the SRE Catalog. Each interface type will reside in the appropriate router.

Exhibit 2.1.6-5. IPS Supported Interface Types (UNI)

UNI Type	Interface	Network-Side Interface	Protocol Type	SRE Interface
1	Cable High Speed Access	320 Kbps up to 150 Mbps	Point-to-Point Protocol, IPv4/v6	[redacted]
2	Ethernet Interface	1. 1 MB up to 1 GbE (Gigabit Ethernet) 2. 10 GbE (Optional) 3. Burstable	IPv4/v6 over Ethernet	1. IPS-2 (1) 2. IPS-2 (2) 3. All Ethernet Interfaces
3	IP over SONET Service	1. OC-3c 2. OC-12c 3. OC-48c 4. OC-192c	IP/PPP over SONET	1. IPS-3(1) 2. IPS-3(2) 3. IPS-3(3) 4. IPS-3(4)
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	1. IPS-4(1) 2. IPS-4(2) 3. IPS-4(3) 4. IPS-4(4) 5. IPS-4(5) 6. IPS-4(6) 7. IPS-4(7)
5	DSL Service (optional)	xDSL access at 1.5 to 8 Mbps downlink, and 384 kbps to 1.5 uplink	Point-to-Point Protocol, IPv4/v6	[redacted]
6	FTTP (optional)		Point-to-Point Protocol, IPv4/v6	[redacted]
7	Wireless Access (optional)	1. LTE 2. Satellite	Point-to-Point Protocol, IPv4/v6	[redacted]

2.1.6.1.7 Performance Metrics [L.29.2.1]

MetTel complies with the requirements for KPI measurement for IPS. MetTel will monitor port availability end to end. [redacted]

Port availability (Av), Latency (CONUS), and GOS (Data Delivery Rate) are all measured and reported historically and in near real time. The Trouble Ticket system maintains Time to Restore (TTR), and MetTel reports TTR on a per-incident basis. All information is available 24x7 to Agencies in the MetTel EIS Portal.

2.1.7 Circuit Switched Voice Service [C.2.2.2]

2.1.7.1 Compliance with Evaluation Criteria [L.29.2.1]

MetTel Anywhere-to-Anywhere
• [redacted]
• Single invoice option to include all invoices across multiple LECs
• Migrating to MetTel does NOT require any changes, no new installations, no porting. Agencies keep everything "as is" with no service interruption
• Unique pricing structure saves money
• Billing and inventory management through user-friendly secure MetTel EIS Portal

MetTel proposes a CSVS solution that meets the mandatory service requirements for CSVS in C.2.2.2. This section presents a technical description of our offering, demonstrating our capabilities in Standards, Connectivity, Technical Capabilities, Features, Performance Metrics, and Interfaces. **Exhibit 2.1.7-1** highlights some key strengths and benefits of our CSVS solution in relation to RFP Section M.2.1 evaluation criteria.

Exhibit 2.1.7-1. Features and Benefits of Approach to CSVS

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• 20 years of experience providing CSVS to industry and Government • [redacted] A combination of local providers and telecommunication giants to deliver CSVS [redacted] • Long distance and international reach equal to the combined reach of all the major long distance providers combined
Quality of Services (M.2.1(2))	• Voice quality at least equal to 64 kbps PCM (standard: ITU G.711) • Network availability 24x7x365 • Transparency and interconnectivity between all providers' networks • [redacted]
Service Coverage (M.2.1(3))	• Global geographic reach through the PSTN • [redacted]
Security (M.2.1(4))	• Compliance with all security and monitoring requirements of the PSTN • Timely access 911 and E911 for emergency service requirements • Support of NS/EP requirements and the Telecommunications Service Priority (TSP) Act

2.1.7.1.1 Service and Functional Description [L.29.2.1, C.2.2.2.1, C.2.2.2.1.1]

MetTel's CSVS provides cost-effective local and long distance solutions for commercial and Government organizations, including in-state, state-to-state, and international calling with plans tailored for all business needs. We offer solutions from basic service to the most advanced features at competitive market rates for basic telephone lines to flat rate, measured, or unlimited local and regional calling plans. Our

plans feature no limitations such as restrictions in calling times or extra digits to dial. Our communications experts identify opportunities to reduce customer costs by eliminating redundancies and recommending latest-technology solutions.

Our model for connectivity links the best price with the best reach to meet CSVS requirements. [redacted] By leveraging multiple access providers, we drive down the price of access and consolidate bandwidth to provide efficiencies that are not available from any single provider.

The Value of Integrated Voice

We migrate and manage telecommunications services for all Agencies under one provider efficiently structured to provide cost-effective, streamlined management and technology migrations, eliminating redundancies and complications of managing multiple service providers. We provide all the required functions, features, and reach of the CSVS requirements and an effective migration path for Agencies seeking the features and functionality of IPVS.

Our solution is developed for the Agency seeking to leverage the advantages of a converged network, including reduced bandwidth, cost savings, and single point of management for multiple vendors, technology, and circuits. We provide the interface, network, and migration path for moving complex CSVS implementation to a cost-effective IPVS solution. Key to our approach, the MetTel EIS Portal is a single information repository for all customer information, including implementation, inventory, maintenance and monitoring, and consolidated billing. Migration is planned and managed to meet Agency operational requirements, facility moves, relocations, and consolidations. [redacted]. We are the only provider capable of managing the complexities of converged networks with a focus on operational efficiencies, reduction in cost, and effective Telecommunications Expense Management (TEM). **Exhibit 2.1.7-2** depicts how MetTel's CSVS and IPVS integration provides total telecommunications management across multiple providers, locations, and technologies.

Exhibit 2.1.7-2. CSVS and IPVS Integration

Quality of Services [L.29.2.1, M.2.1(2)]

We deliver an integrated voice solution for CSVS and work with all the major providers for the best service based on location and Agency requirements. We meet the high expectations of user demands and deliver CSVS to provide high-quality connections across a global geography. We provide voice quality equal to at least 64kbps PCM (standard, ITU G.711) on all calls.

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 U.S. We deliver CSVS functions by combining the assets and reach of our strategic partners to provide a greater reach and connectivity than any partner provider can provide individually.

2.1.7.1.2 Standards [L.29.2.1, C.2.2.2.1.2]

We deliver CSVS in compliance with voice service industry standards.

2.1.7.1.3 Connectivity [L.29.2.1, C.2.2.2.1.3]

MetTel's CSVS is built on the extensive networks of the major local and long distance carriers of PSTN services. MetTel CSVS connects to and interoperates with Government-specified terminations and network terminations defined in **Exhibit 2.1.7-3**

Exhibit 2.1.7-3. CSVS Supported Terminations

Specific Terminations	Network Terminations
Single-line Telephones	Wireline PSTN network
Secure Terminal Equipment	Wireless PSTN network
Multi-line Key Telephone Systems	PSTN domestic
Conference-room Audio Equipment	PSTN non-domestic
PBX	Other EIS voice service networks through the PSTN
Centrex	IPVS
T1 MUX	
Modem	
FAX Equipment	
Video Teleconferencing Systems	
Satellite Phones and Terminals	

2.1.7.1.4 Technical Capabilities [L.29.2.1, C.2.2.2.1.4]

CSVS provides all the technical capabilities required for EIS customers. **Exhibit 2.1.7-4** defines each of the EIS technical capabilities and MetTel's response.

Exhibit 2.1.7-4. CSVS Technical Capabilities

Requirement	MetTel Response
Numbering Plan	a) MetTel provides unique directory numbers for all on-net Government locations, which can be integrated and support existing Government numbers. b) MetTel provides PSTN (both wireline and wireless) numbers and any future changes to PSTN numbers. [redacted] d) MetTel provides transparency and interconnectivity between MetTel networks and the Network Terminations defined in Exhibit 2.1.7-3.
Network Intercept	Network intercept to a recorded announcement is provided as an inherent network capability when a call cannot be completed. Announcements are provided for the following conditions: a) Number disconnected. If MetTel controls the number assignment, we do not reassign the number for 90 days after receiving an Agency disconnect. b) Time-out during dialing typically results in a reorder tone initiated by the switch supporting the station instrument. Switches support this where directly connected station instruments are involved. c) Calls encountering network congestion in the network typically receive a "fast busy" signal. d) On-net originating calls that exceed the class of service assigned to the originating station for off-

Requirement	MetTel Response
	net and non-domestic PSTN calls receive a recorded message stating the call cannot be completed because it exceeds the assigned class of service range privileges. e) MetTel supports the denial of features via class of service restrictions against the originating trunk group, ANI, or authorization code.
User-to-user signaling via ISDN D-Channel (OPTIONAL)	[redacted]
Voice Quality	Voice quality of at least 64 kbps Pulse Code Modulation (PCM) is provided per standard ITU G.711.
911 and E911 Service	MetTel fully complies with emergency service requirements, including 911 and E911 services, identifying the locations of the originating stations and routing them to the appropriate PSAP.

2.1.7.1.5 Features [L.29.2.1, C.2.2.2.2]

CSVS provides the features listed in **Exhibit 2.1.7-5**.

Exhibit 2.1.7-5. CSVS Features

ID Number	Feature	[redacted]
1	Agency-Recorded Message Announcement	
2 (optional)	Authorization Codes/Calling Cards	

ID Number	Feature	[redacted]

ID Number	Feature
3	Caller Identification (ID)
4	Call Screening for users

[redacted]

ID Number	Feature
4.2 (optional)	Call Screening for users (Call Block)
5 (optional)	Customized Network Announcement Intercept Scripts
6 (optional)	Internal Agency Accounting Code
7	Directory Assistance
8	Suppression of Calling Number Delivery
9	Voice Mailbox
10 (optional)	Basic Subscriber Line: Multi-Appearance Directory Number
11 (optional)	ISDN PRI: Back up of Shared-D Channel
12 (optional)	ISDN BRI: Multi-Appearance Directory
13	MLPP

[redacted]

ID Number	Feature	[redacted]
(optional)		

2.1.7.1.6 Interfaces [L.29.2.1, C.2.2.2.3]

We provide all the mandatory interfaces for CSVS. Interfaces to support CSVS depend on the local access provider and availability of the specific interface for the service requested. We bring our large set of LECs, Cable, and Tier-1 providers to deliver the appropriate interface for the requested CSVS service and maintain compliance with all required standards.

2.1.7.1.7 Performance Metrics [L.29.2.1, C.2.2.2.4]

MetTel meets or exceeds the KPIs and AQLs required for CSVS and is a compliant solution that meets all KPIs.

2.1.8 Colocated Hosting Service [C.2.4]

Global, Robust Colocated Hosting Service

[redacted]

- Strategically located robust fiber-rich co-location facilities

The MetTel Team provides compliant Managed Services and co-location solutions for the Federal Government and commercial industries. MetTel provides a comprehensive portfolio of facilities throughout North American, Europe, and Asia [redacted] secure, state-of-the-art co-location infrastructure. Our robust, reliable, fiber-rich co-location facilities are strategically located to provide Agencies with highly-secure and cost-effective options for consolidating existing data center infrastructure and leveraging new IT consumption models such as managed hosting and/or multi-tenant infrastructure services to scale their IT infrastructure and meet their mission requirements.

2.1.8.1 Compliance with Evaluation Criteria [L.29.2.1]

The MetTel CHS solution fulfills the mandatory service requirements as specified in Section C.2.4. This section presents a technical description of our offering, demonstrating our capabilities in standards, connectivity, technical capabilities, features, performance metrics, and security. **Exhibit 2.1.8-1** highlights some key strengths and benefits of our CHS solution.

Exhibit 2.1.8-1. Features and Benefits of Approach to CHS

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• [redacted] • Standards compliant co-location facilities with bandwidth choices • Secure locations with cages, racks, enclosures with state of the art site surveillance
Quality of Services (M.2.1(2))	• MetTel co-location facilities provide robust, reliable compliant services • 24x7x365 live customer support and service monitoring
Service Coverage (M.2.1(3))	• A comprehensive portfolio of facilities throughout North American, Europe, and Asia
Security (M.2.1(4))	• Many choices in type, bandwidth and security of communications to all co-location facilities. • Standard security features include physical protection with guards at each access point, cameras (internal and external), secure locks, mantraps, controlled freight areas and package-handling systems and restricted access to key infrastructure areas

2.1.8.1.1 Service and Functional Description [L.29.2.1, C.2.4.1]

MetTel offers space options from single cabinets to multi-rack cages to private suites. Coupled with configurable primary and redundant power options to support GFP, CHS scales to support Agency near term growth requirements and future expansion. Each cabinet is capable of housing up to 47 rack-unit (RU) worth of equipment and includes secure combination locks for the Agency to control access. External traffic access provides many options with redundancy and choices of circuit type. Internet and other dedicated connection speeds, space requirements, maintenance support and operational support are implemented as specified and approved in an Agency TO.

Cages are designed for Agencies who need the convenience and flexibility of open floor space. Cage environments are built in modular sixty-four square foot (8x8) sections and can be configured to meet Agency growing demands. Cages can accommodate open racks, cabinets, free-standing or non-rack mountable equipment.

For Agencies requiring a higher level of security or larger amounts of floor space, MetTel designs and builds custom suites according to TO requirements. Suites are solid wall structures that restrict visibility and typically add dedicated access security controls such as badge readers. Additional security options include biometric access controls and secure enclosures over the top of the suite and below the floor.

MetTel provides the Government and its representatives with 24x7x365 access to leased space and GFP in the co-location facility. The co-location facilities support the technical capabilities defined in **Exhibit 2.1.8-2**.

Exhibit 2.1.8-2. Co-location Facility Capabilities.

Capability	Met Tel Response
1. Redundant and High-availability power to GFP	MetTel offers configurable primary and redundant power options to run Agency infrastructure in collocated facilities. Primary and secondary power options are available for AC and DC power and are available in several voltage/current circuit configurations.
2. Redundant Uninterruptible Power Supplies (UPS)	Secondary (redundant) power circuits are provisioned to a UPS system that is separate and redundant from the primary power circuit to ensure full redundancy for provisioned power. UPS systems receive power from both commercial power feeds and alternate power sources.
3. Very Early Smoke Detection Apparatus (VESDA)	All co-location facilities are equipped with VESDA systems as part of a comprehensive fire detection and suppression system.
4. Fire Suppression System	All co-location facilities are provisioned with multiple infrastructure elements to ensure timely fire detection and suppression including VESDA throughout the co-location facility. Pre-action dry pipe systems are triggered upon an alert from two sensors, and

Capability	Met Tel Response
	smoke sensors deployed throughout the facilities above the raised floor. Local fire extinguishers are also deployed throughout the facilities and all staff are routinely trained on proper procedures to employ during a fire-related event.
5. Redundant Cooling systems	All co-location facilities are deployed with a redundant N+1 chiller plant to ensure adequate capacity for cooling Agency environments. The overall size/cooling capacity of the chiller plants vary from site to site depending upon the size of the co-location facility.

2.1.8.1.2 Standards [L.29.2.1, C.2.4.2]

MetTel's response to CHS standards are specified in **Exhibit 2.1.8-3**.

Exhibit 2.1.8-3. CHS Standards Requirements

Standards Requirement	MetTel Response
1. TIA-942 Telecommunications Infrastructure Standard for Data Centers (as updated)	TIA-942 Tier 3 standard is our basis for co-location facility design for a continuously maintainable N+1 infrastructure.
2. NIST SP800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations	Multiple co-location facilities have been formally audited and assessed to the Physical and Environmental control standards defined under NIST800-53 rev 4.
3. ICD 705, 26 May 2010, Sensitive Compartmented Information Facilities (as required)	ICD-705 compliant Sensitive Compartmented Information Facilities (SCIF) facilities can be provided upon request in a TO.

2.1.8.1.3 Connectivity [L.29.2.1, C.2.4.3]

MetTel provides exceptional route diversity options and flexible installation schedules to meet Agency requirements specified in a TO. Agencies who need large amounts of bandwidth to conduct their business efficiently will never have to worry about running out of capacity at our co-location facilities. Similarly, Agencies who require exceedingly high communications security have the benefits of selecting from physically diverse routes between their ends points. In short, there are virtually no limitations to the type, amount, or security of communications available at each co-location facility.

2.1.8.1.4 Technical Capabilities [L.29.2.1, C.2.4.4]

MetTel responses to CHS Technical Capabilities are specified in **Exhibit 2.1.9-4**.

Exhibit 2.1.8-4. CHS Technical Capabilities

Technical Capability	MetTel Response
1. At the co-location facility, MetTel is 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	In no event will either party be liable to the other for any type of incidental, special, exemplary, punitive, indirect or consequential damages, including, but not limited to, lost revenue, lost profits, replacement goods, loss of

Technical Capability	MetTel Response
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.	technology, rights to services, loss of data, or interruption or loss of use of service or equipment.
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.	MetTel provides controlled freight areas and package-handling systems to ensure proper delivery and storage of 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.	Remote Hands/Smart Hands services are available to relocate GFP from initial receiving points or temporary storage facilities to final MetTel co-location facility for installation.
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.	MetTel provisions space for CHS to include allocation of physical space, all environmental systems necessary to support the environment, power provisioning, network provisioning and all associated facility systems necessary to maintain the environment on a 24x7x365 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.	MetTel provides Remote Hands/Smart Hands services to facilitate GFP setup, including assembling, loading, configuring and testing. At end of life crating and packing of GFP for return is also provided.
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.	MetTel provides 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.	MetTel provides approved personnel, government and third parties, with the ability to access allocated space and GFP on a 24x7x365 basis at specified times, in specified locations, as mutually agreed upon between the government and the contractor. Access to co-location facilities requires pre-registration of individuals by an authorized Agency representative 48 hours prior to the first access. Presentation of a valid Government-issued identification is required for access to all co-location facilities. All personnel must agree to conform to the MetTel Co-location Facility Policy and the MetTel Acceptable Use Policies (AUP) except where the AUP

Technical Capability	MetTel Response
	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.	Statistics related to power, temperature, entry/exit logs, and other events within the co-location environment are available through the MetTel EIS Portal. Agency personnel are provided access to the MetTel EIS Portal upon establishment of services. Authorized users can access the MetTel EIS Portal remotely.
4. The service management capability shall present alarms to the user in real-time for facility and communication failures.	MetTel provides service alarms to users in real-time for facility and communications failures. Notification are provided via e-mail list, Trouble Ticket notification, or other means as required by a TO.
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.	Statistics related to power, temperature, entry/exit logs, and other events within the co-location environment are available through the MetTel EIS Portal.

2.1.8.1.5 Features [L.29.2.1, C.2.4.5]

The MetTel Team, in collaboration with Raytheon, has experience and supports construction of Sensitive Compartmented Information Facility (SCIF) facilities built to ICD-705 standards. MetTel supports Agency SCIF size and other characteristics as provided in TOs.

2.1.8.1.6 Performance Metrics [L.29.2.1, C.2.4.5.1]

MetTel complies with the performance metrics specified in C.2.4.5.1 for Internet availability and Time to Restore for CHS services.

2.1.9 Wireless Service [C.2.6]

MetTel's Mobile Wireless Service (MWS) for EIS is built on our commercial MetTel Mobile Portfolio of preferred wireless network providers: [redacted] MetTel MWS is a single-source solution that delivers services from the largest national wireless networks to provide converged single bills and a complete set of wireless devices and service plans. This combination provides EIS Agencies reach and connection options that exceed the network of any single provider while providing the dependability of one vendor to ensure all service requirements are delivered from a single trusted source.

MetTel Wireless
Information at Your Fingertips

[redacted]

- Online inventory with Agency Self-Procurement Option and Usage Reports available on the MetTel EIS Portal
- Voice and data plan choices
- Wide selections of everything wireless for connectivity
- [redacted]

2.1.9.1 Compliance with Evaluation Criteria [L.29.2.1]

The MetTel MWS solution fulfills the mandatory service requirements for MWS contained in EIS SOW paragraph C.2.6. This section presents a technical description of our offering, demonstrating our capabilities in Standards, Connectivity, Technical Capabilities, Features, Interfaces, Performance Metrics, and Security. **Exhibit 2.1.8-1** highlights some key strengths and benefits of our MWS solution in relation to RFP section M.2.1 evaluation criteria.

Exhibit 2.1.9-1. Features and Benefits of Approach to MWS

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• Single Government source for access to leading national wireless networks • One dedicated team providing support 24x7x365 • Converged billing of all wireless service for an Agency • [redacted] • Evolution to new technology as soon as it is available in any of the major wireless networks
Quality of Services (M.2.1(2))	• Full compliance with all SOW performance metrics including availability and time-to-restore • 24x7x365 live dedicated customer support • Timely access to the secure MetTel EIS Portal for service information and management
Service Coverage (M.2.1(3))	• [redacted] MetTel's coverage area exceeds that of any single carrier and gives MetTel the largest US Wireless footprint. • Consistent and reliable connectivity with choices of service plans and networks

Evaluation Criteria	Features and Benefits of MetTel's Approach
Security (M.2.1(4))	• Secure voice communications with FIPS 140-2 compliant mobile devices as available • Standards-based and enhanced security to maintain the integrity and privacy of MWS content and collaboration • Supported 3GPP TS 21.133 and LTE-3GPP Release 8 security

2.1.9.1.1 Service and Functional Description [L.29.2.1, C.2.6.1, C.2.6.1.1]

MetTel MWS consolidates access to the nation's leading wireless networks to deliver a broad and powerful range of coverage, even to the most remote locations. Whether Agencies prefer to remain with their existing wireless provider or choose from a diverse set of carriers, [redacted]

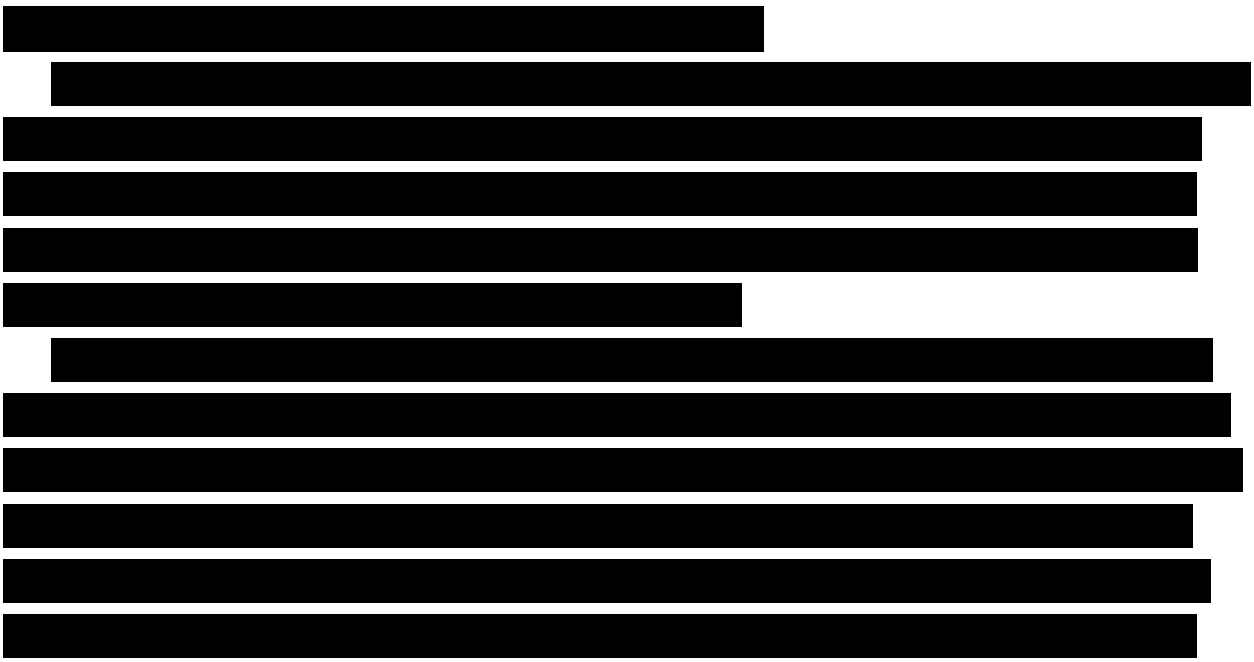
Agencies receive superior coverage, savings, and support from a single provider. MetTel MWS provides access to the leading national and international wireless providers. [redacted]

Many options are available in the mobile market for devices, services, bandwidth, and security. These choices depend on the mobile terminals and technology used in the wireless network and service platforms. MetTel and our wireless providers support older generation technology that is phasing out such as second generation 2G or 2.5G. We work with Agencies to provide the best network to support current and evolving technology, which includes 3G, 4G LTE, and 5G wireless networks in the future. [redacted]

MetTel MWS network partners support Short Messaging Services (SMS), a feature of MWS that provides the capability to send and receive point-to-point or point-to-multipoint text messages on wireless devices. Each SMS message may be up to 160 characters composed of any alphanumeric characters. SMS also supports group messaging via mobile device or website-based entry.

A feature of MWS, Multimedia Messaging Service (MMS) is a standard method for sending messages that include multimedia content to and from mobile phones over a wireless network. MMS allows the transmission of text, audio, images, and video and

extends the core SMS capability that allows exchange of text messages up to 160 characters in length.



2.1.9.1.2 Standards [L.29.2.1, C.2.6.1.2]

MetTel MWS uses the Public Switched Telephone Network (PSTN) and the International Telegraph Union Telecommunication Standardization Sector (ITU-T) standards for interoperability. Wireless providers also adhere to the ITU-T's International Numbering Resources conformance requirements. All of MetTel's domestic providers are members and active participants in the Alliance for Telecommunications Industry Solutions (ATIS) to resolve interoperability issues and use the North American Numbering Plan for call routing and completion.

Our network providers maintain a supporting role in communications standards organizations such as the Cellular Telecommunications and Internet Association (CTIA), which are trade venues that produce the fundamental specifications for the next generation of wireless technology. Introduction of new services and features enables subscribing Agencies to take advantage of the synergies and productivity enhancements of wireless solutions.

MetTel wireless network carriers all support the standards listed in EIS RFP Section C.2.5.1.2. Our network providers are often the leaders in the development and evolution of new wireless standards.

[redacted]

2.1.9.1.3 Connectivity [L.29.2.1, C.2.6.1.3]

Mobile communications today require that the Internet and PSTN be available from all Agency mobile terminals, such as cellular phones, smartphones, wireless-enabled notebooks and laptop, PDAs, and tablets. All MetTel wireless network providers connect to the PSTN and worldwide dialing plan per ITU Recommendation E.164. MetTel MWS originates and terminates calls with users of commercial satellite-based service through the PSTN.

2.1.9.1.4 Technical Capabilities [L.29.2.1, C.2.6.1.4]

MetTel MWS is a full-functional wireless service combining the strength of the major national wireless network providers with the major wireless device vendors. Wireless service supports the capability to originate and receive voice calls from mobile phones, fixed wireline networks, and satellite-based networks through the PSTN. A wide range of devices are available that supports the capabilities defined in C.2.6.1.4, as described in **Exhibit 2.1.9-2**. The wireless device market is rapidly moving, and MetTel provides the current supported models of devices to meet Agency needs. We work with GSA to ensure new devices and technical capabilities roll out to users as rapidly as possible.

Exhibit 2.1.9-2. MetTel MWS Device Capabilities

Mobile Device Type	Capability	[redacted]
a) Cellular Phones	i. Built-in available features	[redacted]
	ii. Wireless broadband devices	[redacted]
	iii. Secure voice communications with FIPS-compliant encryption (as available)	[redacted]
b) Smartphones	i. Built-in available features	[redacted]

Mobile Device Type	Capability	[redacted]
		[redacted]
	ii. Email	[redacted]
	iii. Web browser	[redacted]
	iv. Personal Information Management (PIM)	[redacted]
	v. Sync with leading email, contact/addresses, and calendar platforms	[redacted]
	vi. Vibrate alert to email and text messages	[redacted]
	vii. Ring alert to emails and text messages	[redacted]
	viii. Ability to transfer photos/pictures directly to computer	[redacted]
	ix. Remote kill (as available)	[redacted]
	x. Remote wipe (as available)	[redacted]
	xi. Ability to disable audio, video, and all recording functionality (as available)	[redacted]
	xii. Transmit and receive data (e.g., run an Agency-specific app) while conducting a voice call (as available)	[redacted]

MetTel offers many options in MWS plans and plan aspects for GFP and user-owned devices (BYOD). **Exhibit 2.1.9-3** shows a sample of the MetTel plan options.

Exhibit 2.1.9-3. MetTel MWS Service Plans

Plan Type or Aspect	[redacted]
a) Voice Service Plans	[redacted]
b) Data Add-on Service Plans	[redacted]
c) Data-only Service Plans	[redacted]

Plan Type or Aspect	[redacted]
	[redacted]
d) Machine to Machine (M2M) (optional)	[redacted]
e) Mobility applications for mobile device management (MMS)	[redacted]
f) Mobile Roaming Plans	[redacted]
g) Pooling of domestic data	[redacted]

We comply with Wireless Enhanced 911 (E911) rules including Phase I and II as stipulated by the Federal Communications Commission.

2.1.9.1.5 Features [L.29.2.1, C.2.6.2]

We support all features required in RFP Section C.2.6.2 and define all MetTel MWS features in **Exhibit 2.1.9-4**.

Exhibit 2.1.9-4. MetTel MWS Features

Feature	[redacted]
1. Wireless Priority Service (WPS)	[redacted]
2. Directory Assistance with Call Completion	[redacted]
3. Domestic to Non-Domestic Calling	[redacted]
4. International Mobile Roaming (optional)	[redacted]
5. Personal Hotspot	[redacted]
6. Indoor Cellular Systems	[redacted]
7. Push to Talk with Group Talk	[redacted]

Feature	[redacted]
	[redacted]

2.1.9.1.6 Interfaces [L.29.2.1, C.2.6.3]

We provide devices with all the interface types listed in C.2.6.3.1. The type of interface available and the network that supports the Interface Standard are specifically available from some or all of our wireless network providers. [redacted]

2.1.9.1.7 Performance Metrics [L.29.2.1, C.2.6.4]

[redacted]

2.1.10 Unified Communications Service [C.2.8.3]

MetTel has a unique position in the telecommunications industry as an organization built as an integrator of telecommunications services. Many legacy voice vendors view unified communications as add-on functionality to core telephony, whereas MetTel believes unified communication is the next evolution of telephony and provides UC solutions that treat voice, video, messaging, and collaboration as a unified application and not separate islands with obligatory interoperability. [redacted]

UCS
The future of Communication

- Unified applications for voice, video and messaging
- [redacted]
- Many device choices phones, tablets, computers
- Fraud protection and role based access controls

[redacted]

The MetTel UCS solution for EIS includes a scalable solution with flexibility to meet future requirements, and meet program goals including service continuity, high quality service and operations support. [redacted]

2.1.10.1 Compliance with Evaluation Criteria [L.29.2.1]

The MetTel UCS solution fulfills the mandatory service requirements for UCS contained in SOW paragraph C.2.8.3. This section presents a technical description of our offering, demonstrating our capabilities in the following areas: Standards,

Connectivity, Technical Capabilities, Interfaces, Performance Metrics, and Security. **Exhibit 2.1.10-1** highlights some key strengths and benefits of our UCS solution in relation to RFP section M.2.1 evaluation criteria.

Exhibit 2.1.10-1. Features and Benefits of Approach to UCS.

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• [redacted] • EIS will benefit from MetTel industry expertise and premium customer service, integrated in the MetTel EIS portal • Collaboration across voice (CSVS or IPVS), and applications including unified messaging, instant messaging, presence, voice mail, integration with email where applicable, and FAX allowing users access to messages with any device, anywhere and at any time.
Quality of Services (M.2.1(2))	• Full compliance with all SOW performance metrics (see Section 2.1.11.1.7) • 24×7 live customer support and online trouble management • Agencies have timely access to secure MetTel EIS portal for service ordering, trouble management, inventory control and service billing. • [redacted]
Service Coverage (M.2.1(3))	• [redacted] • Global geographic coverage for both voice and data access for users to access the UCS functionality
Security (M.2.1(4)	• Single sign on capabilities through the agency's Enterprise Active Directory (EAD) system. • Role Based Access Controls implemented • [redacted]

2.1.10.1.1 Service and Functional Description [L.29.2.1, C.2.8.3.1, C.2.8.3.1.1]

MetTel has multiple methods for fulfilling EIS UCS program goals. Both on premises and network-based service solutions combine independently-run communications subsystems in order to streamline how agency's users and customers communicate and collaborate regardless of location. [redacted] 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.

[redacted]

MetTel UCS software services are a fully-managed service that delivers comprehensive unified communications services from MetTel's embedded network infrastructure. UCS wraps its unified communications applications with a fully-managed, end-to-end operating platform, accessible through the MetTel EIS Portal, supporting the full life cycle for the Agency customer, from initial provisioning, service activation, and customer service. By managing the end-to-end customer initiation and service implementation process, UCS significantly reduces an enterprise's internal development and infrastructure investments.

[redacted]

MetTel understands integration of new solutions requires transition planning and experience with similar size and scope implementations. MetTel has the experience and capabilities for Agencies today and seamless growth and enhancement for the future.

[redacted]

2.1.10.1.2 Standards [L.29.2.1, C.2.8.3.1.2]

The MetTel UCS platform operates on a standards-based, modular architecture that uses common protocols (such as Session Initiation Protocol [SIP]), open interfaces, and scalable, industry-standard hardware. The open environment enables users to provide user services, administrative features, and media-based functionality from a standards-based service delivery platform. UCS functionality is distributed across multiple servers and locations for optimized performance and reliability.

The MetTel unified UCS complies with all EIS minimum standards as listed in **Exhibit 2.1.10-3** below:

Exhibit 2.1.10-3. Standards Response and Discussion.

Standard Requirements	Compliant	[redacted]
IETF RFC Standards for IP-based voice, data, and video applications.	Yes	[redacted]
SIP/SDP	Yes	[redacted]
SRTP & G.711/G.722/G.729/H.264/OPUS CODEC, IETF RFC 6716 CODEC	Yes	[redacted]
DSCP and LLDP	Yes	[redacted]
TLS and MTLS	Yes	[redacted]
ICE/STUN/TURN	Yes	[redacted]
XMPP/SIP/PIDF	Yes	[redacted]

Additionally, MetTel will comply with specific standards as identified in a TO and other appropriate standards for any applicable underlying EIS access and transport services.

2.1.10.1.3 Connectivity [L.29.2.1, C.2.8.3.1.3]

UCS connects to and interoperates with the PSTN through SIP trunk gateways and agency communications subsystems such as voice, email, conferencing (audio, web-based video), instant messaging, presence, and collaboration portals, over an IP network whether agency provided or contractor provided.

[redacted]

MetTel's SIP trunk solution, defined in Section 2.1.3.1.9 delivers SIP Trunks which are fully compliant with the current SIP Connect 1.1 standard. [redacted]

2.1.10.1.4 Technical Capabilities [L.29.2.1, C.2.8.3.1.4]

MetTel's UCS offers the government a variety of communications options to support program initiatives and strategic goals. Our UCS solution brings all real-time

communications services together into one convenient communication application accessible from desktop phones, mobile devices (smart phones, tablets, etc.), wireline and IP phones, soft clients, and video conferencing devices. UCS supports both IPv4, IPv6 and is able to communicate over IPv4-only, IPv6-only, and/or dual stack networks.

[redacted]

Exhibit 2.1.10-4 provides the MetTel response to the UCS requirements for Unified Messaging.

Exhibit 2.1.10-4. Unified Messaging (UM) Capabilities.

Technical Capability	Compliant	[redacted]
a) User access and management of voice mail, e-mail and fax messages through the same inbox or interface.	Yes	[redacted]
b) Modular messaging with access to messages from phones and PC's via various interfaces, including browsers	Yes	[redacted]
c) UC Messaging Directory	Yes	[redacted]
d) UC Messaging Directory Objects	Yes	[redacted]

Technical Capability	Compliant	[redacted]
		[redacted]

Exhibit 2.1.10-5 defines the Mobile Integration Capabilities provided by UCS. Many of these capabilities are provided through IPVS in conjunction with UCS capabilities.

Exhibit 2.1.10-5. Mobile Integration Capabilities.

Technical Capability	Compliant	[redacted]
a) Single Identity	Yes	[redacted]
b) Call forwarding to any phone using a single number for making and receiving all calls.	Yes	[redacted]
c) Hand off calls from cellular to Wi-Fi connections and vice versa on smart phones	Yes	[redacted]
d) Enable user to initiate phone call, retrieve voice mail, corporate directories, access instant messaging and participate in video conferencing.	Yes	[redacted]
e) Provide features that are access ble 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.	Yes	[redacted]
f) Allow calls to or from mobile devices to take place anywhere and anytime as if they are to/from the desk phone numbers.	Yes	[redacted]

Exhibit 2.1.10-6 provides the MetTel response to the Unified User Interface capabilities. [redacted]

Exhibit 2.1.10-6. Unified User Interface.

Technical Capability	Compliant	[redacted]
a) The ability for users to access UC capabilities from a variety of devices in a variety of ways.	Yes	[redacted]
b) Features such as presence, instant messaging, integrated soft phones, voice conferencing, video	Yes	[redacted]

Technical Capability	Compliant	[redacted]
calling and conferencing.		[redacted]
c) Voice activation that integrates seamlessly with other business communication systems.	Yes	[redacted]
d) Real-time communications – instant messaging, presence that identifies which participant is speaking, voice calls to video, voice calls to email.	Yes	[redacted]
e) Non-real time communications – email, text messaging, fax, voice mail.	Yes	[redacted]
f) Collaboration and data sharing – electronic bulletin boards, e-Calendar, Audio/Video/Web conferencing.	Yes	[redacted]
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	Yes	[redacted]
h) Instant messaging between two users or multiparty (up to an agency-defined number of participants).	Yes	[redacted]
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.	Yes	[redacted]
j) Presence integration with agency collaboration applications, such as calendaring, that automatically updates presence when users are in a meeting.	Yes	[redacted]
k) Audio and video conversations between two users or multiparty (up to an agency-defined number of participants), using web cameras, speakers and microphones.	Yes	[redacted]
l) File Transfer capabilities to send files between	Yes	[redacted]

Technical Capability	Compliant	[redacted]
users.		[redacted]
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.	Yes	[redacted]
n) Contact Groups that allow users to organize their contacts	Yes	[redacted]
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.	Yes	[redacted]
p) Agency-managed instant messaging administration (add/change/delete users).	Yes	[redacted]
q) Single sign-in capabilities through the agency's Enterprise Active Directory (EAD) system.	Yes	[redacted]
r) Automated and/or staffed UCS-dedicated Service Desk available 24/7.	Yes	[redacted]

MetTel UCS supports UC deployments by providing Instant Messaging and

[redacted]

[redacted]

[redacted]

[redacted]

Quality of Service

MetTel implements, supports and honors QoS markings and implementation over the MetTel MPLS core network that are used to access the UCS. [redacted]

[redacted]

[redacted]

IPv4 and IPv6

MetTel UCS solution supports both IPv4 and IPv6 and will be able to communicate over IPv4-only, IPv6 only, and/or dual-stack networks. MetTel supports GSA initiatives to simultaneously process IPv4 and IPv6 traffic. We can also leverage Dual Stack

network to migrate IPv4 to IPv6 for future requirements.

2.1.10.1.5 Features [L.29.2.1, C.2.8.3.2]

There are no Features listed for UCS.

2.1.10.1.6 Interfaces [L.29.2.1, C.2.8.3.3]

MetTel UCS is based on open standards, which makes it highly interoperable and supportable on different devices, including IP Phones, Mobile Phones, Web Browser, Email Clients, Desktop Clients, PCs and Tablets. [redacted]

[redacted]

2.1.10.1.7 Performance Metrics [L.29.2.1, C.2.8.3.4]

[redacted]

MetTel will meet or exceed the KPI's for availability and Time to restore for the UCS service. Trouble management is managed through the MetTel EIS portal and the EIS Help Desk.

[redacted]

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 [redacted]

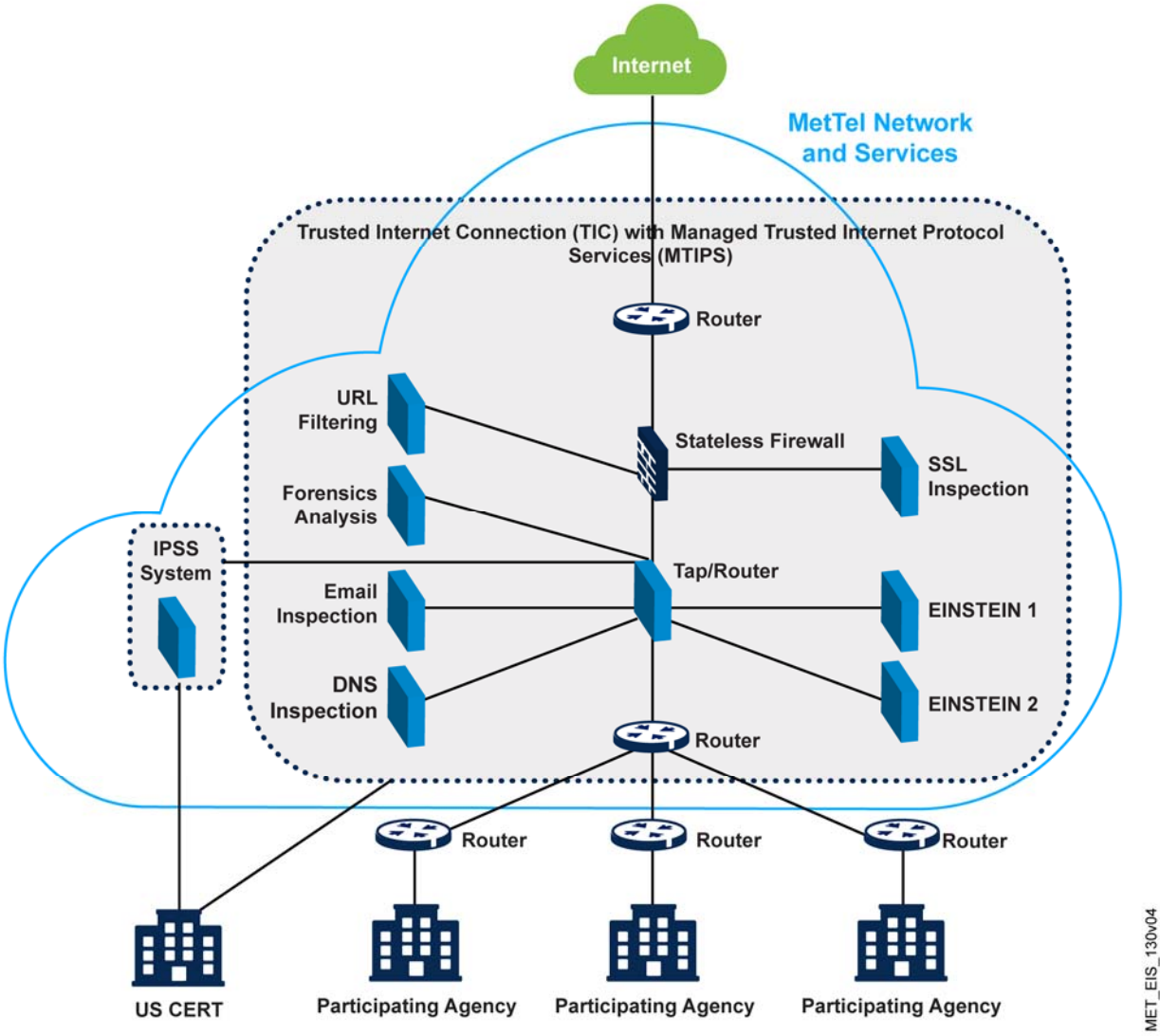


Exhibit 2.1.11-1 MTIPS Configuration and High Level Data Flow

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.

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]
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]

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.

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

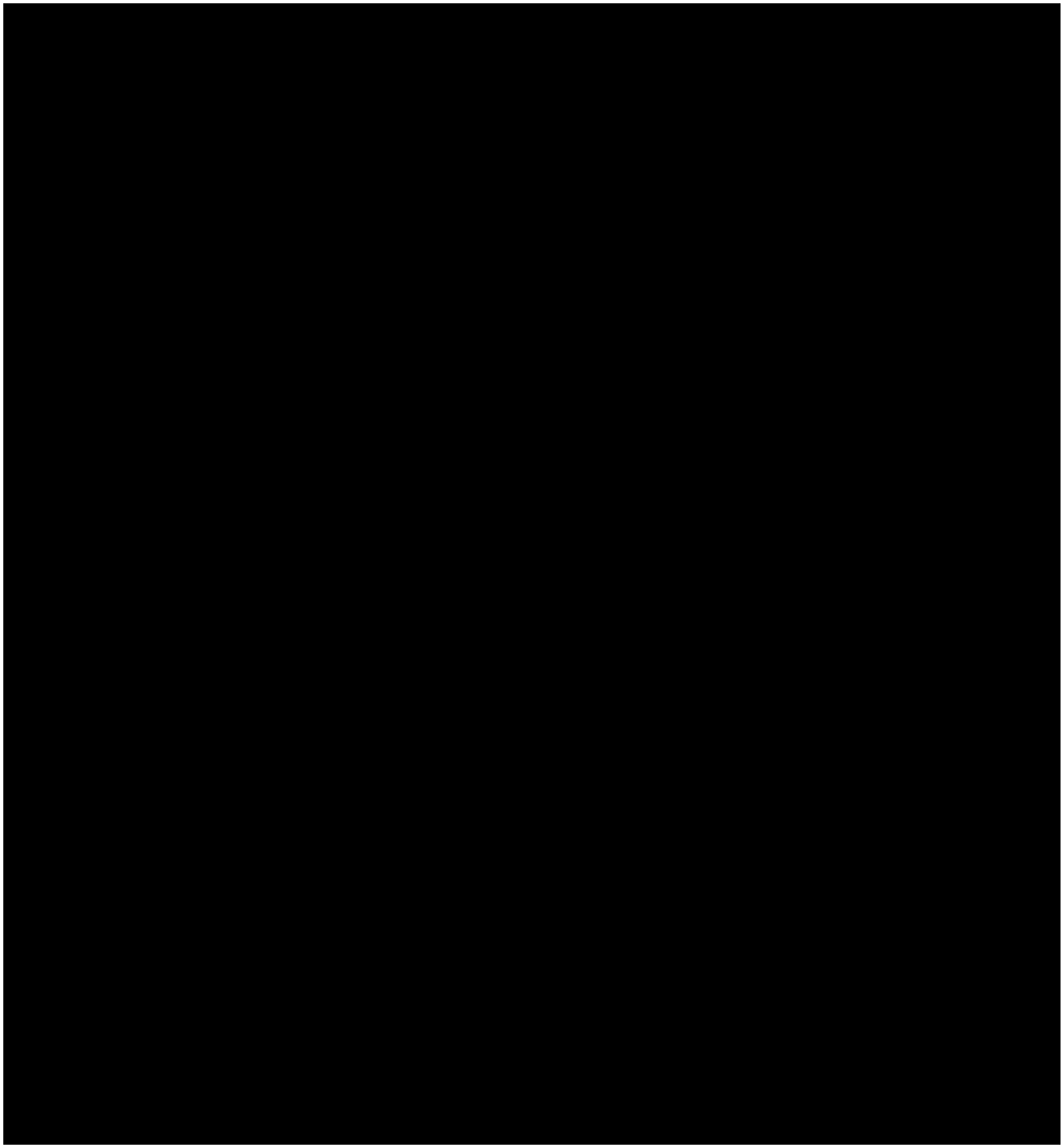


Exhibit 2.1.11-6. TIC and MTIPS connections to PA's

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 for SONET [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	
		Within 30 minutes of a High category event	≤ 30 minutes	

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	

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

2.1.12 Managed Security Service [C.2.8.5]

Our teammate, Raytheon Company ("Raytheon"), provides the Managed Security Service (MSS) to meet the requirements for the EIS program and Foreground, recently acquired by Raytheon, will provide tools and SOC services. Agencies must keep up with today's increasingly formidable cyber threats, as cybercriminals and corrupt organizations grow in sophistication and number. To combat these threats, a combination of automated and human-driven solutions are necessary to establish always-alert, hypervigilant positioning for incident anticipation, discovery, response, and mitigation. Raytheon's MSS provides EIS with Managed Prevention Services (MPS), Vulnerability Scanning Services (VSS), and Incident Response Services (INRS) to safeguard Agency internal networks and systems against ever-evolving security threats.

2.1.12.1 Compliance with Evaluation Criteria [L.29.2.1]

Raytheon's MSS solution fulfills the mandatory service requirements for MSS defined in SOW paragraph C.2.8.5. The following section presents a technical description of our offering, demonstrating our capabilities in Standards, Connectivity, Technical Capabilities, Features, Performance Metrics, and Security. **Exhibit 2.1.12-1** highlights some key strengths and benefits of our MSS solution.

Exhibit 2.1.12-1. Features and Benefits of the Raytheon Solution

Evaluation Criteria	Features and Benefits of Raytheon's Approach
Understanding (M.2.1(1))	• The requirements outlined in the SOW correspond with the MSS Raytheon has provided to multiple Government Agencies. • Raytheon has integrated managed prevention solutions into multiple Government Agencies (cited in QOS below) and commercial clients and monitors the installed solutions via the Raytheon Virtual SOC (V-SOC) in Herndon, Virginia. • Raytheon has successfully applied [redacted] in analyzing and reporting the security posture of client computer and network environments qualitatively and quantitatively improving their security posture • Raytheon's incident response programs are developed and integrated into the client business operations and have been at the forefront of remediating large scale agency and industry breeches
Quality of Services (M.2.1(2))	• Raytheon's extensive Government support has allowed us to tailor our MSS approach for supporting [redacted]

Evaluation Criteria	Features and Benefits of Raytheon's Approach
	[redacted] etc. • These Government Agencies have provided us with numerous commendations and excellent reviews when directly interacting with key Government Agency personnel.
Service Coverage (M.2.1(3))	• MetTel provides MSS in the top 100 [redacted], CONUS, and OCONUS.
Security (M.2.1(4))	• Raytheon delivers remote managed [redacted] • We access [redacted] • Raytheon utilizes a [redacted] • Our blended MSS team comprises experienced TS/SCI cleared analysts and engineers who are available as "smart hands" to support DHS supplied equipment. • The MSS team works in concert with our NOC and is [redacted]

2.1.12.1.1 Service and Functional Description [L.29.2.1, C.2.8.5.1, C.2.8.5.1.1]

Raytheon's MSS [redacted] he tools utilized by our MSS include, but are not limited to, [redacted] Our MSS model automates much of the signature-based network security tools through our patented [redacted]

Our MSS offering includes the following benefits on a 24x7x365 basis:

- Security monitoring and analysis support to investigate threats identified through our MPS, VSS, and INRS
- Full management, content development, integration, and engineering key security tools including Agency edge routers
- Active advanced detection and threat "hunting" through a combination of our [redacted]
- DFIR support for compromised systems and network attacks

As depicted in **Exhibit 2.1.12-2**, Raytheon's MSS ties the MPS, VSS, and INRS together into a living and breathing lifecycle that continually increases the MSS's human and machine learning and its overall capability to protect against security threats. The products (output) of one service are ingested into the other services for [redacted] **Exhibit 2.1.12-3** shows the metrics displayed on the client interface of [redacted]

Exhibit 2.1.12-2. Raytheon's MSS

Exhibit 2.1.12-3. Raytheon's [redacted] Client Interface

Raytheon provides the services to design, implement, sustain, manage and monitor diverse MPS systems and components that secure department and agency infrastructures. Our MPS model is further designed to provide all inputs, data points, and updates necessary to support an enterprise incident management capability. We work with Agency staff [redacted]

Raytheon's VSS model is designed to [redacted]. Risks are evaluated according to requirements for compliance as determined by Agency standards. VSS also detects [redacted] We examine the [redacted] We then [redacted] Information from VSS is fed back [redacted]

Raytheon's INRS model is designed to [redacted] We understand the complexities of how to skillfully navigate in

"crisis mode." We integrate with Agency POCs to [redacted] We perform [redacted] to ensure incidents are not repeated.

The [redacted] platform [redacted] Content from [redacted] investigations or incidents [redacted] to support enterprise workflow.

Once the determination has been made that an incident is occurring or has occurred, our analysts [redacted] Understanding where and when to utilize these standard Agency processes is a major part of [redacted]

[redacted]

2.1.12.1.2 Standards [L.29.2.1, C.2.8.5.1.2]

MSS complies with all the appropriate standards for any underlying EIS access and transport service and the specific standards and requirements identified in an Agency Task Order as required in C.2.8.5.1.2.

2.1.12.1.3 Connectivity [L.29.2.1, C.2.8.5.1.3]

MSS connects to and interoperates with the Agency networking environment, including Demilitarized Zones (DMZs) and secure LANs, as required by the Agency. MSS also supports connectivity to Extranets and the Internet and ensures seamless connectivity to Agency networking environments as specified in C.2.8.5.1.3.

2.1.12.1.4 Technical Capabilities [L.29.2.1, C.2.8.5.1.4]

Raytheon's team leverages an integrative approach to develop and provide MPS, VSS, and INRS. Our MSS fuses [redacted]

We [redacted] referenced in **Exhibit 2.1.12-5**.

Exhibit 2.1.12-5. Raytheon's MSS Flow

Custom content is what drives the advanced capabilities offered in our Security Analytics. Our team maintains

2.1.12.1.4.1 Managed Prevention Service (MPS) [C.2.8.5.1.4.1]

In support of MPS, the Raytheon team provides enterprise As part of our MPS turnkey capability, Raytheon Security Engineers These components are designed and rigorously tested to meet, or exceed, network performance KPIs and Agency functionality requirements. Following design and testing, our team the appropriate Agency-specific data. As part of on-going management, in accordance with our focus on continuous service improvement, our team

[redacted] are the core of the successful SOC and MSS business we provide to numerous Federal Agencies. Our team [redacted] Raytheon maintains a [redacted].

Our management approach is aligned to industry best practices such as ITILv3 for Service Management. This approach guides MPS and dictates rigorous testing and deployment processes, detailed outage reporting and root cause analysis, and continuous service improvement. At a tactical level, Raytheon's staff [redacted] Finally, we make available to the Agency all service related data including, but not limited to, [redacted]

2.1.12.1.4.2 Vulnerability Scanning Service (VSS) [C.2.8.5.1.4.2]

Raytheon's MSS uses a standard, [redacted] (shown in **Exhibit 2.1.12-6**) for our VSS that tests [redacted]

[redacted]

Exhibit 2.1.12-6. Raytheon's Four Phase Vulnerability Testing Methodology

Scoping

Scoping involves gathering general information (see **Exhibit 2.1.12-7**) via the following sources and methods:

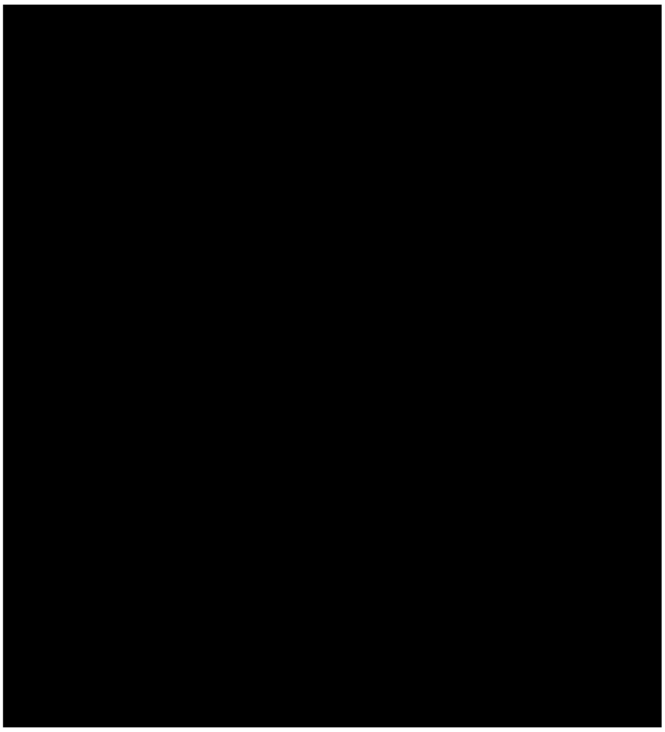


Exhibit 2.1.12-7. Scoping

Reconnaissance

This phase consists of profiling the target environment (see **Exhibit 2.1.12-8**) Some of the steps taken in this phase of target discovery and target enumeration include:

Exhibit 2.1.12-8. Profiling Target Environment

[redacted]

Multiple commercial and open source tools may be used during this phase, including those listed in **Exhibit 2.1.12-9** commonly used by Raytheon:

Exhibit 2.1.12-9. Commonly Used Tools

[redacted]

Testing

In this phase, the MSS analysts [redacted] In cases where an individual finding has an exceptionally large number of potentially affected hosts, [redacted] **Exhibit 2.1.12-10** displays some of the key components to the Raytheon testing phase. The MSS analysts:

[redacted]

Exhibit 2.1.12-10. Testing Phase

[redacted]

In the event of a test with rules of engagement permissive to exploitation,

[redacted]

[redacted] with the Agency's permission, some may be exploited as a proof of concept.

Reporting

The reporting phase shown in **Exhibit 2.1.12-11** proactively notifies the agency of [redacted]

[redacted]

Exhibit 2.1.12-11. Reporting Phase

[redacted] with the Agency's own risk acceptance policy. The reports create a clear understanding and correlation of:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Risk Assessment

During the activation phase, a [redacted] to define [redacted] are detected. The Raytheon team works with the Agency to [redacted]

2.1.12.1.4.3 Incident Response Service (INRS) [C.2.8.5.1.4.3]

Raytheon's MSS Incident Response Service provides [redacted] that are key to the Agency's continued cyber security success.

Incident Response Preparation and Planning

The most successful incident response programs are developed and integrated into business operations well in advance of a security incident. As part of the INRS, Raytheon MSS [redacted]

Raytheon's MSS also provides an [redacted]

Incident Response and Management Services

Under the INRS, Agencies receive priority access to Raytheon's MSS analysts and Subject Matter Experts (SMEs). Key elements of this support include:

- [redacted]

When a potential security incident is identified, Raytheon's MSS SMEs [redacted]

[redacted] to minimize exploitation of Agency assets. [redacted] . Our MSS [redacted] the successful remediation of any vulnerabilities.

Our MSS INRS team [redacted] subject to direction by authorized Agency personnel. The Agency may request documentation and case notes at any stage of this response process.

Service Level Objectives

For the INRS, Raytheon's MSS SLA objective is a [redacted]

Core Capabilities

Our activities are performed in such a manner to [redacted] **Exhibit 2.1.12-12** lists key INRS capabilities.

Exhibit 2.1.12-12. Raytheon INRS Capabilities

[redacted]

[redacted]

As part of Raytheon's MSS, we act as part of the Agency's [redacted] Our incident reporting includes [redacted]

From the time of discovery, [redacted] We provide the Agency team the ability to trace each incident response lifecycle and participate [redacted]

To facilitate [redacted] Each of the content elements denoted under each step of the incident handling methodology play a critical role in said incident handling methodology detailed in **Exhibit 2.1.12-13**. [redacted]

[redacted]

Exhibit 2.1.12-13. Raytheon INRS Handling Methodology

2.1.12.1.5 Features [L.29.2.1, C.2.8.5.2]

Raytheon's MPS provides the features listed in **Exhibit 2.1.11-14**.

Exhibit 2.1.12-14. Raytheon MPS Features

[redacted]

[redacted]

Raytheon's MSS [redacted] as requested by the Agency and [redacted] One of the differentiating

factors for Raytheon's VSS is [redacted] space for active attacks; [redacted] Our seasoned INRS personnel have [redacted] Our methods for uncovering evidence of compromise or validating false positives do not change and are [redacted] While not analyzing during an active incident, [redacted]

2.1.12.1.6 Interfaces [L.29.2.1, C.2.8.5.3]

The Raytheon MSS supports the interfaces of VPNS, ETS, and IPS without issue when integrated within the customer environment due to the autonomy of the MSS.

2.1.12.1.7 Performance Metrics [L.29.2.1, C.2.8.5.4]

We meet or exceed the values of the KPIs for MSS and all underlying EIS security services we manage.

Raytheon supports all performance metrics for our MSS as specified in the Task Order. In addition to the MetTel EIS Portal, the [redacted]

2.1.13 Managed Mobility Service [C.2.8.6]

[redacted]

- Satisfies strict Government security standards and FISMA compliance
- FIPS 140-2 and AES 256 compliant
- Flexible deployment options built to scale with growing Agency requirements
- Containerized solutions to protect Government data, applications, email, and browsing on employee-owned devices (BYOD)

[redacted] Our management solutions enable organizations to securely manage large-scale deployments of mobile devices, [redacted] from a single web-based console.

[redacted] Combined with the extensive inventory and telecommunications expense management capabilities of the MetTel EIS Portal, the Agency has all the information necessary to effectively and efficiently manage the complete network, wireline and wireless.

2.1.13.1 Compliance with Evaluation Criteria [L.29.2.1]

The MetTel MMS solution fulfills the mandatory service requirements for MMS C.2.8.6. This section presents a technical description of our offering, demonstrating our capabilities in Standards, Connectivity, Technical Capabilities, Features, Performance Metrics, and Security. **Exhibit 2.1.13-1** highlights some key strengths and benefits of our MMS solution.

Exhibit 2.1.13-1. Features and Benefits of Approach to MMS

Evaluation Criteria	[redacted]
Understanding (M.2.1(1))	
Quality of Services (M.2.1(2))	
Service Coverage (M.2.1(3))	
Security (M.2.1(4))	

2.1.13.1.1 Service and Functional Description [L.29.2.1, C.2.8.6.1, C.2.8.6.1.1]

MMS helps Agencies 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 many Agencies focus more on BYOD initiatives and advanced wireless computing.

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. The optimal balance between security, total costs, and functionality provides the most business value to Agencies.

[redacted]

Functional Description

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, and deployment support.

- Agencies **configure MMS** in conformance to security policies, ensuring the mobile device fleet is compliant regardless of device ownership (i.e., BYOD)

- MMS makes it **easy to deploy** secure MDM, MAM, MCM solutions for the entire Agency device fleet

2.1.13.1.2 Standards [L.29.2.1, C.2.8.6.1.2]

MetTel MMS complies with all the following standards:

FISMA Moderate Impact level standards –

2. **NIST 800-53** – The MetTel MMS Information Security Program is modeled using industry best practices and regulatory standards, including NIST SP 800-53 which typically aligns with customer policies and programs.

FIPS-140-2 – is fully FIPS 140-2 compliant,

4. **IPv4 and IPv6** – MMS supports both IPv4 and IPv6 addressing.

5. **Specific standards as identified in a Task Order –** [redacted]

2.1.13.1.3 Connectivity [L.29.2.1, C.2.8.6.1.3]

Our MMS solution is carrier/network agnostic and simply requires a network connection to function. MMS is supported over all MetTel preferred wireless networks and our preferred global partners and supports all major smartphone and tablet OSs, [redacted] MMS is interoperable with Wi-Fi network connections.

2.1.13.1.4 Technical Capabilities [L.29.2.1, C.2.8.6.1.4]

MMS capabilities are subdivided into:

- Mobile Device Management
- Mobile Application Management
- Mobile Content Management
- Mobile Security
- Deployment Support

The following subsections describe the requirements for each of these areas.

2.1.13.1.4.1 Mobile Device Management [C.2.8.6.1.4.1]

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. MMS MDM enables Agencies to address challenges associated with mobility by providing a simplified, efficient way to view and manage devices from the central administrator console function. [redacted] **Exhibit 2.1.13-2** defines MDM capabilities for MSS.

Exhibit 2.1.13-2. MDM Capabilities of MMS [redacted]

MDM Capabilities	[redacted]
a) Enforce enterprise rules	[redacted]

MDM Capabilities	[redacted]
b) Actions upon groups	
c) Assign Profiles to one or many Groups	
d) Mobile Applications Store (MAS)	
e) View and run reports	
f) Run reports by group of users to include locations	
g) Software Development Kit or API Framework	
h) Monitor MDM with industry standard tools	
i) Integrate PKI certificates	
j) Perform MDM functions from within a VPN	

Device enrollment is a key capability to ensure the MMS enforces Agency policies. **Exhibit 2.1.13-3** identifies the elements available when adding a device to the MDM management domain in the MMS.

Exhibit 2.1.13-3. MDM Device Enrollment Capabilities

Capabilities	Compliant
a) Set a Target Platform	Yes
b) Use a Target Device Model for profile	Yes
c) Specify minimum OS version	Yes
d) Target Device Ownership	Yes
e) Allow a user to edit any field for a "live" or "active" profile	Yes
f) Allow a user to self-enroll an Agency GFP or BYOD device	Yes
g) Centrally manage multiple devices	Yes
h) Support different policies or grouping for multiple devices under one user	Yes
i) Apply multiple policies to devices simultaneously	Yes
j) Use external directory service repository for enrollment.	Yes
k) Use federated and multi-factor authentication for enrollment	Yes
l) Set support email and phone information for registration messages	Yes
m) Redirect users to a URL upon successful enrollment	Yes
n) Edit an enrollment activation notification message to user	Yes
o) Set a default Device Ownership type upon enrollment for different groups	Yes
p) Use an internal user list for enrollment for different groups	Yes
q) Set support email and phone information for registration messages for different groups	Yes
r) Edit an enrollment activation notification message to the user or group of users	Yes

Capabilities	Compliant	[redacted]
s) Send a user or group an activation enrollment message	Yes	

Device profiles define users and group capabilities in the MMS and are key to enforcing Agency policies. [redacted] **Exhibit 2.1.13-4** defines the requirements for device profiles and MetTel's response.

Exhibit 2.1.13-4. MMS Device Profiles

Capabilities	Compliant	[redacted]
a) Create a profile template	Yes	
b) Copy profiles	Yes	
c) Edit a "live" or "active" profile	Yes	
d) Set profile removal permissions	Yes	
e) Set Profile Start Date	Yes	
f) Set Profile End Date	Yes	
g) Automatically update a device that currently has a profile when editing that profile	Yes	
h) Push a profile to an individual device	Yes	
i) Automatically remove profiles from devices whose state changes from qualifying to not-qualifying	Yes	
j) Support multiple profiles being applied to a single device (most restrictive rules apply)	Yes	
k) Delete a profile from the MDM system	Yes	
l) Set a description for a profile	Yes	
m)Manage the following via a profile:		
i. Install applications	Yes	
ii. Control use of camera	Yes	
iii. Control use of installed applications, including default applications	Yes	
iv. Allow multiple Wi-Fi configurations for a single profile	Yes	
v. Manage device Wi-Fi settings via a MDM policy	Yes	
vi. Control Wi-Fi Security Type	Yes	

Capabilities	Compliant
vii. Multiple VPN configurations for a single profile	Yes
viii. VPN Connection (or Policy) Type	Yes
ix. VPN Connection Proxy for a VPN configuration	Yes
x. Multiple email/calendar/contact configurations per profile	Yes
xi. Multiple Web Clip / Web Shortcut configurations per profile	Yes

[redacted]

Device feature management provides control of the features in devices and the flexibility to enable or disable specific features. **Exhibit 2.1.13-5** defines the required set of device feature management capabilities.

Exhibit 2.1.13-5. MMS Device Feature Management Capabilities

Capabilities	Complia
a) Multi-OS support – Manage multiple OS devices	Yes
b) Device passcode enforcement (complexity, length, presence)	Yes
c) Installation of applications (See MAM)	Yes
d) Camera (enable/disable)	Yes
e) Control radios/communications	Yes
i. Wi-Fi (enable/disable)	Yes
ii. Bluetooth (enable/disable)	Yes
iii. Enable or disable specific hardware component and uses	Yes
iv. Near Field Communications (NFC) (enable/disable)	Yes
v. Enable/disable GPS	Yes
vi. Store Enterprise/Agency data to removable media (disable)	Yes

[redacted]

MDM provides a robust set of additional management capabilities for an Agency to control the mobile fleet as required to meet operational requirements. **Exhibit 2.1.13-6** provides the MetTel response to the required MDM capabilities.

Exhibit 2.1.13-6. Additional MDM Capabilities

Capabilities	Compliant
5. Data Management – read, write, transmit, and receive data on mobile devices as well as with backend systems/repositories	Yes
a) File Management – to secure data, files, and applications (e.g., pdf files or Word docs) on a mobile device	Yes
b) Personal Information Management	Yes
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	Yes
7. Device Inventory Management and Reports	Yes
8. System Performance Reports	Yes
9. MDM Security/Compliance Reports	Yes
10. Capabilities that may be defined in the Task Order:	
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.	Yes, optional
b) (Optional) Classified Data – shall support access classified data up to the SECRET level via mobile devices.	Yes, optional

[redacted]

Capabilities	Compliant
c) (Optional) PIV/CAC Support – shall support the management of PIV/CAC cards on mobile devices via the MDM	Yes, optional
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.	Yes, optional
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).	Yes, optional

[redacted]

2.1.13.1.4.2 Mobile Application Management [C.2.8.6.1.4.2]

Mobile applications are changing the way people work. Mobile users demand applications that connect them to enterprise resources, increase their productivity, and promote collaboration with colleagues. [redacted]

MAM capabilities include Application Deployment, MAS, Application Security, and some optional capabilities that may be defined at the Task Order level. MetTel MMS is fully compliant with these requirements. **Exhibit 2.1.13-7** through **Exhibit 2.1.13-10** define the MetTel response to MAM capabilities.

Exhibit 2.1.13-7. Application Deployment

Capabilities	Compliant
a) Commercial Application Store	Yes
b) Reporting of installed applications	Yes
c) Block Application Purchase	Yes
d) Application Whitelisting/Blacklisting	Yes
e) Staged/controlled application deployment.	Yes

[redacted]

The MAM provides the user the ability to select private enterprise or Agency applications for installation on managed devices. MAS is integrated into the MDM on the MetTel EIS Portal and allows application provisioning by group policy and mandatory application deployment. MAS supports the capabilities defined in **Exhibit 2.1.13-8**.

Exhibit 2.1.13-8. Mobile Application Store

Capabilities	Compliant
i. Add/update an application from a Commercial Application Store to the MAS	Yes
ii. Add additional metadata to and report on metadata on any application added to the MAS (name, description, version, OS, keywords, etc.)	Yes
iii. Add/update an enterprise/Agency application to the MAS via a web GUI	Yes
iv. Specify the effective date for an Agency internal application	Yes
v. Specify the expiration date for an Agency internal application	Yes
vi. Specify the minimum operating system and model for an Agency internal application	Yes
vii. Download Agency internal and public applications from MAS	Yes
viii. Categorize, group, or tag applications (e.g., business applications, scientific applications, etc.)	Yes

[redacted]

Application Security provides the capability to approve applications for operation and protect the applications on the wireless device as a key element of the overall MAM. **Exhibit 2.1.13-9** lists MDM Application Security capabilities.

Exhibit 2.1.13-9. MAM Application Security

Capabilities	Compliant
a) Mutual Authentication	Yes
b) Application Installation Control	Yes
c) Blacklisting / Whitelisting	Yes
d) Application Environment Requirements – detect and enforce device environment conditions such as:	Yes
i. Minimum or specific operating system versions	Yes
ii. Required presence or absence of other applications	Yes
iii. Absence of privilege escalation (“rooting” or “jai breaking”)	Yes

[redacted]

Capabilities	Compliant	
e) Application Signing – shall support requiring digital signatures for application installation from both commercial and private application stores and direct application push / deployment	Yes	[redacted]

An Agency may define optional capabilities in a Task Order. **Exhibit 2.1.13-10** defines MAM optional capabilities.

Exhibit 2.1.13-10. MAM Optional Capabilities

Capabilities	Compliant	
a) Third-party Application Mutual Authentication to provide third-party applications with mutual authentication and secure communications through wrappers, binary patching, etc.		[redacted]
b) MAM Software Integration Services	Yes	

2.1.13.1.4.3 Mobile Content Management [C.2.8.6.1.4.3]

[redacted]

[redacted]

Accessible, round-the-clock mobile connectivity drives modern enterprise productivity. The proliferation of consumer mobility drives demand for a simple and ubiquitous content collaboration solution. [redacted] These integrated solutions empower the mobile workforce and provide unprecedented innovation and networking without compromising data security and granular control.

MCM enables secure mobile access to content anytime, anywhere, and on any device. MCM protects sensitive content and provides a central application to securely access, store, update, and distribute documents. Mobile Security and Deployment Support are the key elements of MCM and are defined in the following sections.

2.1.13.1.4.4 Mobile Security [C.2.8.6.1.4.4]

Exhibit 2.1.13-11 provides the MetTel response to the requirements for Mobile Security defined in EIS RFP Section C.2.8.6.1.4.4. The MetTel MMS solution [redacted] complies with all mobile security requirements in this section.

Exhibit 2.1.13-11. Mobile Security Capabilities of MMS

Capabilities	Compliant
1. Enroll a device before applying any policy (null Policy)	Yes
2. Create Whitelists/Blacklists for device enrollment to include OS versions and device models	Yes
3. Allow enrollment of untrusted devices and anonymous / unknown users outside the enterprise as individuals or to groups under the MDM	Yes
4. Use an existing MDM user attribute repository for enrollment to the new MDM system	Yes
5. Take action based on compliance rules	Yes
6. Block the device or erase (wipe) only the managed data on a device under the following conditions:	
a) Blacklisted	Yes
b) Exceed a set number of failed login attempts	Yes
c) Exceed defined interval for contacting MDM (policy based)	Yes
d) Detection of OS jailbreaking or application tampering (policy based)	Yes
e) Any other policy violation	Yes

[redacted]

Capabilities	Compliant
f) Remote instruction from MDM (manual)	Yes
7. Password policy enforcement:	
a) Minimum complexity (length, composition, common words, etc.)	Yes
b) Password lifetime limit	Yes
c) Password re-use limits	Yes
d) Password inactivity timeout	Yes
e) Report password failures beyond threshold to MDM	Yes
f) Maximum password attempts before lock or wipe	Yes
8. Mask passwords when they appear in the Management GUI	Yes
9. Determine which administrative user made a configuration change in the MDM administrative environment	Yes
10. Determine which device user made a configuration change in the MDM console (self-service logging)	Yes
11. Installation and configuration (update, revocation checking) of individual and group authentication certificates for the following purposes:	Yes
a) Email (S/MIME) signing and encryption	Yes
b) Wi-Fi Configuration	Yes
c) VPN Configuration	Yes
12. Send/receive (encrypt and sign, decrypt and verify)	Yes
13. Restrict downloading attachments, copying of data to/from removable media	Yes
14. (Optional) View the current GPS location of a device or logical grouping of devices on a map	Yes
15. Encrypt the data in transit between the MDM and the device in accordance with FIPS 140-2	Yes
16. Data at rest on a mobile device	Yes
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:	Yes
a) Shared Secret	Yes

Capabilities	Compliant
b) Token	Yes
c) Biometric	Yes
18. User Compliance:	
a) Set up compliance rules to include custom compliance rules for profiles, devices, groups, and Whitelist/Blacklist	Yes
b) Activate/deactivate a compliance rule	Yes
c) Specify user and group rules for application	Yes
d) Provide enterprise-level compliance reports	Yes
19. Alerting – notify Agency operations staff about Agency devices:	
a) Set up custom alerts to users and management based on various parameters	Yes
b) Send custom alerts to one or more user roles including administrators	Yes
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	Yes
e) Create alerts based on device status such as battery low, device roaming, equipment down (not responding), device inactive, etc.	Yes
f) View alerts pending acknowledgement	Yes
g) Acknowledge alerts and track acknowledgements	Yes
20. Audit reports – as defined in a Task Order:	Yes
a) Administrator activity (i.e., actions performed, time stamps)	Yes
b) User access times and enrollments	Yes
c) Devices (i.e., number of devices by Agency and across all sub-Agencies, type, OS version)	Yes
d) Console logins and functions (connections to the management console, actions performed, etc.)	Yes
e) Policy changes and versions (policy revision control and historical changes)	Yes
f) Policy violations	Yes
21. Safeguard any Personally Identifiable Information (PII), including directory data stored in the information system in accordance with NIST SP 800-122	Yes

Capabilities	Compliant	[redacted]

2.1.13.1.4.5 Deployment Support [C.2.8.6.1.4.5]

End user experience across multiple components (i.e., laptops, tablets, and smartphones) has been difficult and disruptive in the past. As mobile technology evolves, users demand a consistent experience across all devices. Our MMS platform provides leading enterprise-grade solutions across every device, every operating system, and every mobile deployment. [redacted]

Exhibit 2.1.13-12 summarizes deployment options with the MetTel MMS solution.

Exhibit 2.1.13-12. Mobile Deployment Support

[redacted]

The MetTel MMS solution provides deployment capabilities in full compliance with the EIS RFP stated capabilities.

1. Deployment

MetTel provides a comprehensive implementation package [redacted] Initially, our team assesses requirements, consults on options, demonstrates capabilities, and assists with other project needs. Whatever the mobile enterprise requirements, we provide personalized and professional consultation services to ensure our solution addresses key mobility concerns. A consultant works with users to build out the project plan with specific milestones and deliverables including assisting the Agency with accreditation and authorization (compliance) objectives. MMS supports integration with existing enterprise infrastructures and systems.

We understand the importance of industry standards [redacted] Our due

diligence demonstrates our commitment to preserve the confidentiality, integrity, and availability of data while implementing appropriate security measures and monitoring systems. The MMS data center operations team leverages a documented methodology encompassing configuration, capacity, change, service level, availability, and incident and problem management policies and processes.

2. Enterprise System Integration

MetTel assists with deploying and integrating MMS into the Agency-wide environment. We securely integrate with Active Directory (AD) and Lightweight Directory Access Protocol (LDAP), certificate authorities, email infrastructures, and other enterprise systems in a cloud and on-premise deployment model to preserve the Agency investment in existing enterprise resources, centralize mobility management, and streamline user enablement. We integrate Trouble Ticketing with the MetTel EIS Portal to provide enterprise-wide trouble management and reporting.

3. Training

MetTel provides MDM and MAM solution training materials, online training, and additional training resources. [redacted]

4. Help Desk

The MetTel EIS Help Desk provides MDM and MAM support for all EIS users and Agencies. Users initiate support for trouble request and resolution via email or telephone or by creating an online Trouble Ticket.

2.1.13.1.5 Features [L.29.2.1, C.2.8.6.2]

No features are specified for MMS.

2.1.13.1.6 Interfaces [L.29.2.1, C.2.8.6.3]

MetTel MMS supports UNIs for all smartphones and tablets running smartphone operating systems across 3G/4G Cellular Service based on CDMA, GSM, and LTE standards as required. The SRE Catalogue lists all SREs with the designation “Wireless” in the Note column.

2.1.13.1.7 Performance Metrics [L.29.2.1, C.2.8.6.4]

The MetTel EIS Portal supports the EIS Services Trouble Management System (TMS). All KPIs for MMS are met and reported through the TMS. Users can query the status of Trouble Tickets and their status against the KPIs and performance thresholds. The TMS complies with the event notification values and the severity they indicate.

2.1.14 DHS Intrusion Prevention Security Service [C.2.8.9]

MetTel IPSS
• Compliant, scalable, reliable, and resilient solution • Incremental IPSS implementation capability • Extens ble approach to add future DHS EINSTEIN Enclave features

The Department of Homeland Security (DHS), Office of Cybersecurity and Communications (CS&C), is partnering with select Internet Service Providers (ISP) to provide support for the Einstein 3-Accelerated (E3A) program. The E3A program provides protection from Advanced Persistent Threats (APT) to Internet traffic either destined to, or originating from federal civilian Executive Branch participating Departments and Agencies (PA), commonly referred to as ".gov" traffic. The Intrusion Prevention Security Service (IPSS) is at the core of the E3A program; providing the integrated cyber appliances needed to meet E3A objectives.

The MetTel IPSS solution fulfills the mandatory service requirements for the IPSS in SOW paragraph C.2.8.9. It will provide a continuous monitoring environment including the application of intrusion prevention capabilities of Participating Agency approved agency traffic. The service will be based upon guidance received from the U.S. Department of Homeland Security (DHS) National Cyber Security Division (NCSD), Director of National Intelligence, NIST, industry standards, and MetTel best practices. Additionally, the IPSS extensible environment can be enhanced in compliance with future developments as they evolve.

Upon becoming an MTIPS provider, MetTel intends, with DHS approval and support, to participate in the Einstein program as a provider. With the assistance of Raytheon Company (Raytheon), we will establish an accredited TS/SCI Sensitive Compartmented Information Facility (SCIF) E3A Enclave and implement the functions of the E3A program for the IPSS capability. The MetTel Team offers an expandable and extensible architecture capable of providing all capabilities identified in the 5 March 2013 IPSS Statement of Objectives (SOO).

[redacted]

[redacted]

2.1.14.1 Compliance with Evaluation Criteria [L.29.2.1]

The MetTel IPSS solution fulfills the mandatory service requirements for IPSS in C.2.8.9. It is nominally sized to support 10 Gbps throughput. 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 2.1.14-1** highlights some key strengths and benefits of our IPSS solution in relation to RFP Section M.2.1 evaluation criteria.

Exhibit 2.1.14-1. Features and Benefits of Approach to IPSS

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• MetTel's teammate Raytheon, a cybersecurity leader for more than 30 years, developing and deploying technologies that keep Enterprises through Nation States attacks safe. Raytheon has expanded their industry-leading capabilities through over $5 billion invested in 17 acquisitions in the past ten years. Its focus on Cyber Security has made it a worldwide leader in defensive cyber security systems. • Intranet, Extranet, and remote access using industry-standard protocols such as IPsec and TLS across properly sized access methods. • Secure VPNs that are based on IPSec, cryptographic algorithms, and industry-standard authentication methods and that transverse trusted VPNs or Internet Protocol Service (IPS) • Architecture is extens ble to enable new protocols.
Quality of Services (M.2.1(2))	• Full compliance with all SOW performance metrics including performance metrics specified in future task orders

Evaluation Criteria	Features and Benefits of MetTel's Approach
	• Scalable architecture enables addition of future capabilities [redacted] • Resilient – The IPSS components that comprise the IPSS are designed to fail open (no blockage of data)
Service Coverage (M.2.1(3))	• None, RFP Section B.1.2.1.1, Pricing Identification Structure specifies CBSA does not apply to IPSS.
Security (M.2.1(4))	• IPSS operates within a secure environment that assures availability, confidentiality, and integrity of the network traffic being monitored and processed. • Compliance with the IPSS Security Requirements Traceability Matrix (SRTM) that are derived from NIST SP 800-53v4. • IPSS components are designed to fail "open"; no data is prevented from passing through. • [redacted]

2.1.14.1.1 Functional Description [L.29.2.1, C.2.8.9.1, C.2.8.9.1.1]

[redacted]

Functional System Design Overview

[redacted]

Assumptions

[redacted]

[redacted]

Core Infrastructure

[redacted]

[redacted]

Core Infrastructure IPSS Concept of Operations

Per the IPSS requirements, we provide the ability to capture and store packet and other analytically relevant data [redacted]

Alerting and Reporting

[redacted]

Overall, Raytheon's Core Infrastructure Service solution meets all DHS and MetTel requirements while providing flexibility to expand to a highly available architecture and integrate future capabilities.

Performance Specification

Initial design capacity is driven by PA service level agreements (SLA). Latency (DNS) is dictated by system processing latency and physical displacement. [redacted]

System Design Detail

This section provides a detailed overview of our solution, describing each component and its function. All components were selected after detailed trade studies.

Firewall

[redacted]

[redacted]

Event Logging Event Capture & Storage

[redacted]

System Monitoring

[redacted]

DNS IPSS Concept of Operations (Blocking, Sink-holing)

[redacted]

[redacted]

DNS Detection/ DNS Alert Response / Blocking / Sinkhole

[redacted]

[redacted]

E-Mail (SMTP) Processing

[redacted]

[redacted]

Secure Environment

[redacted]

[redacted]

Indicator and Signature Management

[redacted]

2.1.14.1.2 Standards [L.29.2.1, C.2.8.9.1.2]

MetTel's partner, Raytheon, is a commercial service provider participant in the DHS Enhanced Cybersecurity System (ECS) program. Performance and security requirements and standards are similar to IPSS. Raytheon's experience will be leveraged to expeditiously implement IPSS.

Applicable Regulations, Policies, and Instructions

MetTel understands the importance of providing a fully compliant system that not only adheres to government standards but also provides assurance that information

security and privacy concerns remain paramount. Our solution ensures a low-risk transition to operations based on the current version of NIST SP 800-53v4, "Recommended Security Controls for Federal Information Systems," the current version of NIST SP 800-37, NIST SP 800-64 "Security Considerations in the Information System Development Life Cycle," and FIPS PUB. In addition, [redacted]

Verification & Validation

Verification and validation is subdivided into three categories: *Developmental* which confirms correct implementation of a new capability; *Assessment and Accreditation* which confirms the security and hardening of the IPSS; and *Operational* which confirms the correct functioning of signatures and indicators within the IPSS. DHS NCSD and DHS I&A are invited to observe or participate in any developmental capability testing or operational signature testing. Test reports will be available for review and concurrence.

Developmental

With each increment of the component integration and configuration, testers, independent of the network engineer, will conduct component or product-level testing. The testers will create test cases that are traceable to all requirements in the system specification and SRTM. Once a network engineer completes and verifies a requirement, the designated tester will develop and execute a test case. As new functionality is added to the baseline, the tester performs regression tests to ensure that newly integrated capabilities do not affect existing functionality. Any discovered non-conformances will be entered into the defect tracking tool, fixed by the development team, and validated by the tester. The testers will also create test data sets and configure the test harnesses as required to allow verification of all requirements.

MetTel is responsible for injecting the test data sets into the systems under test. If any non-conformances are discovered, they will be documented and fixed by the technical team in order to complete checkout verification.

Assessment & Authorization

Following verification of functionality, a Raytheon and MetTel technical team will prepare the system for acceptance test and assessment and authorization (A&A) activities. Raytheon will assist MetTel to provide inputs to a set of security artifacts that are used by the government to assess the security posture of the services provided by the contractor. This includes, but may not be limited to: Security Concept of Operations (SECONOPs), an Architectural overview, Standard Operating Procedures (SOP), System configurations for all devices performing security-relevant functions, including configurations of all security-related software, an SRTM Response, Vulnerability and penetration test results, incident reports (or templates) used to detail any security incidents already experienced on the system, and if applicable, source code for custom code developed, including modifications to commercial or open-source programs, and a Plan of Action and Milestones (POA&M) that identifies security findings and associated plans to remediate those findings.

Typical preparations include clearing out all logs, and configuring the system to a candidate set of PA parameters that MetTel has agreed to with DHS for acceptance testing. The Raytheon technical team will perform dry runs of the acceptance test cases to ensure the IPSS system is ready for acceptance testing.

In support of the certification and accreditation, Raytheon will support technical assessments including testing of controls, system penetration testing, and security compliance reviews and audits. We will also support development of mitigation plans for open findings. This phase ends when the IPSS systems have been accredited and MetTel has received an ATO.

Operational

As part of the IPSS delivery, MetTel will provide a Service Verification Environment (SVE). The SVE complements the operational IPSS and is a form-fit-function identical instantiation of the IPSS. The purpose of the SVE is to confirm the proper functionality of signatures under simulated, representative traffic prior to upload to the IPSS.

2.1.14.1.3 Connectivity [L.29.2.1, C.2.8.9.1.3]

[redacted]

[redacted]

2.1.14.1.4 Technical Capabilities [L.29.2.1, C.2.8.9.1.4]

Exhibit 2.1.14-5. Required Technical Capabilities

Requirement	[redacted]
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 poss ble.	
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	

Requirement	[redacted]
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	

Requirement	
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 United States Computer Emergency Readiness Team (US-CERT).	
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	

Requirement	[redacted]
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 US-CERT 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	

Requirement	
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.	[redacted]

2.1.14.2 Features [L.29.2.1, C.2.8.9.2]

[redacted]

2.1.14.3 Interfaces [L.29.2.1, C.2.8.9.3]

[redacted]

2.1.14.4 Performance Metrics [L.29.2.1, C.2.8.9.4]

The representative architecture in this section is designed to be modified to meet latency, capacity, availability, reliability, and protocol metrics as defined in individual TO.

2.1.15 Service Related Equipment [C.2.10, Section D]

2.1.15.1 Compliance with Evaluation Criteria [L.29.2.1]

The MetTel SRE solution fulfills the mandatory service requirements for SRE contained in SOW paragraph C.2.10. This section presents a technical description of our offering, demonstrating our capabilities in the following areas: Standards, Connectivity, Technical Capabilities, Features, Performance Metrics, and Security. **Exhibit 2.15-1** highlights some key strengths and benefits of our SRE solution in relation to RFP section M.2.1 evaluation criteria.

Exhibit 2.1.15-1. Features and Benefits of Approach to SRE.

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• MetTel provides hardware to agencies for 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. • MetTel provides hardware and materials that are incidental to the installation, operation and maintenance of EIS services.
Quality of Services (M.2.1(2))	• All MetTel equipment provided to the government under this contract shall be new and not previously used or refurbished. • 24x7 live customer support and monitoring of shipments • Packaging and packing shall comply with the requirements of the Uniform Freight Classification and the National Motor Freight Classification (issue in effect at time of shipment) and each shipping container or each item in a shipment shall be of uniform size and content, except for residual quantities. Where special or unusual packing is specified in a task order, but not specifically provided for by the contract, such packing details must be agreed to by the ordering agency and the contractor.
Service Coverage (M.2.1(3))	• MetTel will 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.
Security (M.2.1(4)	• All leased equipment, accessories, and devices located on government property shall be dismantled and removed from government premises by the contractor, at the contractor's expense, within 45 days after the service termination date. • Advance notice must be provided to the Local Government Contact to ensure that dismantling and removal occurs with a minimum of disruption. Exceptions to this requirement shall be mutually agreed upon and written notice issued by the agency Ordering Contracting Officer (OCO).

Understanding [L.29.2.1, M.2.1(1)]

MetTel will provide hardware and materials that are incidental to the installation, operation and maintenance of EIS services. MetTel provides 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.

All equipment provided to the government under EIS will be new and not previously used or refurbished. This hardware and materials are incidental to the installation, operation and maintenance of EIS services. Unless otherwise specified, all items shall be preserved, packaged, and packed in accordance with normal commercial practices, as defined in the applicable commodity specification. Packaging and packing will comply with the requirements of the Uniform Freight Classification and the National Motor Freight Classification (issue in effect at time of shipment) and each shipping container or each item in a shipment will be of uniform size and content, except for residual quantities. Where special or unusual packing is specified in a task order (TO), but not specifically provided for by the contract, such packing details must be agreed to by the ordering agency and MetTel.

A packing list or other suitable shipping document will accompany each shipment and will indicate:

1. Name and address of the consignor
2. Name and complete address of the consignee
3. Government order or requisition number
4. Government bill of lading number covering the shipment (if any)
5. Description of the material shipped, including item number, quantity, number of containers, package number (if any), and weight of each package

All initial packing, marking and storage incidental to shipping of equipment to be provided under EIS will be MetTel's expense. Such packing, supervision marking and storage costs will not be billed to the government. Supervision of packing and unpacking of initially acquired equipment will be furnished by the MetTel.

All leased equipment, accessories, and devices located on government property will be dismantled and removed from government premises by MetTel, at the MetTel's expense, within 45 days after the service termination date. All dismantling and removal of equipment is performed by the MetTel during normal government business hours at the location. Advance notice must be provided to the Local Government Contact to ensure that such dismantling and removal occurs with a minimum of disruption to any service or operation. Exceptions to this requirement will be mutually agreed upon and written notice issued by the agency Ordering Contracting Officer (OCO).

Quality of Services [L.29.2.1, M.2.1(2)]

MetTel provides a minimum of one year system warranty (or provided by the manufacturer) for all hardware and software ordered under EIS, including all equipment supplied, installed, and integrated by MetTel. The MetTel equipment warranty provides for hardware repairs and the distribution of updated software to all users who ordered the hardware and software under the EIS contract. MetTel provides warranty information associated with each product and service delivered to the GSA CO or OCO.

MetTel will repair or replace malfunctioning equipment covered by warranty within five (5) business days or as specified in the TO. A MetTel point of contact will be identified and available from 7 AM to 7 PM local time or for a longer period as specified in the agency TO. Warranty begins at the time the SRE is accepted.

MetTel has strict policies that all equipment has been purchased from reputable vendors who provide certificates of authenticity and warranties for all the equipment and components they provide. These certificates and warranties are passed along to the customer as part of the MetTel sales agreement.

Additionally, MetTel only works with Original Equipment Manufacturers (OEMs) that exercise strict quality control to ensure that counterfeit or illegally modified hardware or software components are not incorporated into the OEM product and include traceability and evidence of genuineness of Information Technology Tools (ITT) back to the licensed product and component OEMs.

MetTel corporate policy ensures that SCRM clauses are inserted into all purchasing agreements with vendors and that the vendors supply us with the appropriate SCRM documentation as specified in NIST SP 800-161. MetTel maintains full documentation

and audit trails with all of our vendors to ensure full accountability throughout the purchasing and acquisition lifecycle.

Service Coverage (for CBSA-dependent services) [L.29.2.1, M.2.1(3)]

MetTel equipment will be provisioned in the awarded CBSA's as requested in the agency TO.

Security [L.29.2.1, M.2.1(4)]

MetTel does not purchase anything or enter into contractual relationships with unknown and/or unidentified sources under any circumstances. Our corporate reputation depends on our integrity and the integrity of our supply chains.

MetTel policy for Enterprise System and Services Acquisition defines MetTel policy for managing risks from third party components and services' providers. Through the establishment of an effective third party risk management program, MetTel implements security best practices with regard to Systems and Services Acquisition and Supply Chain Risk Management.

2.1.15.1.1 Warranty Service [L.29.2.1, C.2.10.1]

MetTel provides, 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 EIS, including all equipment supplied, installed, and integrated by MetTel. The equipment warranty shall provide for hardware repairs and the distribution of updated software to all users who ordered the hardware or software under EIS. MetTel provides 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.

MetTel strictly follows our System and Services Acquisition Policy and our SCRM Policy which mandates purchasing solely from publically known sources who provide genuine "brand name" hardware and software complete with warranties, certifications, and support, which are then passed to the agency/end-user.

MetTel conducts a supplier review process which is strictly policy based prior to entering into a contractual agreement to acquire COTS software. MetTel inserts SCRM clauses into all our contracts to ensure that our vendors are contractually obligated to comply with our SCRM requirements.

MetTel requires that all hardware and software products purchased, come complete with vendor certification and warranties. We maintain an automated system which tracks software licensing to ensure that MetTel is in full compliance with all hardware and software licensing requirements.

2.1.16 Service Related Labor [C.2.11, B.2.11.2; J.5; J.9; J.10]

The MetTel Service Related Labor (SRL) fulfills the mandatory requirements for SRL contained in SOW paragraph C.2.1.21. This section presents a technical description of our offering, demonstrating our capabilities to provide qualified labor as requested in a TO. **Exhibit 2.1.16-1** highlights some key strengths and benefits of our SRL solution in relation to RFP section M.2.1 evaluation criteria.

MetTel Service Related Labor
• MetTel supports all SRL categories and levels • MetTel's qualified candidate pool meets or exceeds technical expertise and skill requirements across all Labor Categories • MetTel assures timely availability of qualified, suitable staff to support new TO requirements • MetTel's candidate pool possess requiste security clearances

Exhibit 2.1.16-1. Features and Benefits of Approach to SRL.

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• SRL is labor required 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. • SRL is not to implement the mandatory or optional services in this proposal.
Quality of Services (M.2.1(2))	• MetTel provides labor categories defined in J.5 of the EIS RFP • MetTel provided labor categories are further subdivided into three levels: Junior, Journeyman, and Senior / Subject Matter Expert (SME), based on years of experience and duties/responsibilities.
Service Coverage (M.2.1(3))	• SRL will be provided at SDPs and facilities that are supported by the SDP and agency requirements defined in the Agency TO.
Security (M.2.1(4)	• MetTel SRL will meet any requirements specified in the TO for proof of citizenship or security clearance.

MetTel services proposed for EIS include all service-related labor necessary to implement the service. In cases where Agencies request labor in a TO for support services such as construction, alteration, and repair and these services are within the scope necessary for a complete solution, MetTel provides the scope and cost of labor using the site survey templates provided in J.9 and J.10. In these cases, the SRL is considered integral to and necessary for the effort defined in the TO.

Labor Categories and Levels

[redacted] supports all labor categories and levels required by the EIS RFP in B.2.11.2 and J.5. [redacted]

[redacted]

Job Levels

Labor categories are further subdivided into three levels in accordance with RFP Section B.2.11.2: Junior, Journeyman, and Senior / Subject Matter Expert (SME), based on years of experience and duties/responsibilities as follows:

- JUNIOR: An individual in the junior labor category level has up to 3 years of applicable experience. Such an individual is responsible for assisting more senior positions and/or performing functional duties under the oversight of more senior positions.
- JOURNEYMAN: An individual in the Journeyman labor category level has 3 to 10 years of applicable experience. Such an individual typically performs all functional duties independently.
- SENIOR/SME: An individual in the Senior / Subject Matter Expert (SME) labor category has more than 10 years of applicable experience, or is an individual whose qualifications or expertise are exceptional, or is recognized as an industry leader for a given area of expertise. Such an individual performs all functional duties independently, and may oversee the efforts of less senior staff and/or be responsible for the efforts of all staff assigned to a specific job.

2.1.17 Cable and Wiring [C.2.12, J.9]

The MetTel Cable and Wiring (CW) solution fulfills the mandatory service requirements for CW contained in SOW paragraph C.2.12. This section presents a technical description of our offering. **Exhibit 2.1.17-1** highlights some key strengths and benefits of our CW solution in relation to RFP section M.2.1 evaluation criteria.

Exhibit 2.1.17-1. Features and Benefits of Approach to CW.

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• [redacted] providing Cable and Wiring to industry and Government • Local labor that knows the building codes and regulations to satisfy the local jurisdiction and government building requirements. • All staff have required certifications to comply with appropriate standards.
Quality of Services (M.2.1(2))	• MetTel provides a one (1) year warranty period on all premise wiring/cabling after the service has been accepted by the CO or OCO. • 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. • All planned work and code compliance shall be subject to OCO review and approval prior to the start of work.
Service Coverage (M.2.1(3))	• MetTel cable and wiring is available whereever an EIS service is required. • The government will furnish facilities and utilities to the contractor that already are installed at the site, including light, heat, ventilation, and power. MetTel will provide temporary utilities that are not available in the work area and coordinate any disconnection of utilities. MetTel will 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.
Security (M.2.1(4)	• MetTel will comply with all citizenship, back ground investigation or security clearances required in a TO.

MetTel has teams of local contractors that will provide installation services for equipment necessary to provide telecommunications services and related supporting IT services on a per TO basis. MetTel uses local contractors to provide required connectivity using appropriate cabling and wiring, and related trenching, ducting, grounding, and lightning protection systems in accordance with the TO and appropriate local codes and standards. All site preparation work performed by MetTel will conform to applicable federal, regional and local codes and will conform to accepted industry installation and construction practices. MetTel will use the Site Survey Estimate Template for Wiring Install (Table J.9 of the EIS RFP) to provide detail estimate of cost for all CW tasks defined in a TO.

All planned work and code compliance will be reviewed and approved by the OCO and the local building approval authority prior to start of work. MetTel and our team of contractors will provide the tools and test equipment to perform the site preparation as specified in the TO. Ownership of all tools and test equipment will be retained by MetTel and its contractors unless otherwise specified in the TO.

MetTel understands that the government will furnish facilities and utilities to MetTel that already are installed at the site, including light, heat, ventilation, and power. MetTel will provide temporary utilities that are not available in the work area and coordinate any disconnection of utilities required to implement new services.

MetTel will provide building additions or changes to the existing structure to support the telecommunications and IT installation that are integral to and necessary for the effort defined in the TO. HVAC and electrical construction will be limited to new or upgraded installations necessary to support telecommunications and IT equipment. MetTel will expand or enhance power systems to provide appropriate environmental controls to support the installation and requirements of the TO.

MetTel will use the Site Survey Estimate Template for Wiring Install provided in J.6 of the EIS RFP for defining the scope and cost of each site defined in the TO. Each site survey will include the completed Template and any necessary drawings or pictures to support the efforts required to implement the telecommunications and IT services. MetTel will provide a warranty period of at least one (1) year for the premises wiring/cabling after the service has been accepted by the CO or OCO.

2.1.18 Toll Free Service [C.2.2.3]

2.1.18.1 Compliance with Evaluation Criteria [L.29.2.1]

MetTel proposes a Toll Free Service (TFS) solution that meets the mandatory service requirements for TFS in C.2.2.3. This section presents a technical description of our offering, demonstrating our capabilities in Standards, Connectivity, Technical Capabilities, Features, Performance Metrics, and Interfaces. **Exhibit 2.1.18-1** highlights some key strengths and benefits of our TFS solution in relation to RFP Section M.2.1 evaluation criteria.

Exhibit 2.1.18-1. Features and Benefits of Approach to TFS

[redacted]

Agencies can use MetTel's inbound 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.

MetTel's 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.

2.1.18.3 Standards [L.29.2.1, C.2.2.3.2]

MetTel's TFS complies with the standards shown in Exhibit 2.1.18-2. MetTel's voice service engineers maintain awareness of new and changing industry and government standards that may impact our TFS solution. We update our TFS service accordingly to ensure GSA and all clients have the advantage of new features, capabilities and functions that new and changing standards make possible. For GSA and Agencies, this results in a TFS that is always up-to-date and avoids technology obsolescence and ensuring that future growth is addressed.

Exhibit 2.1.18-2: MetTel's Support of Required Standards

[redacted]

2.1.18.4 Connectivity [L.29.2.1, C.2.2.3.1.3]

MetTel's TFS connects to and interoperates with the Public Switched Telephone Network (PSTN) including wireline and wireless networks. Our TFS utilizes the underlying CSVS and IPVS [redacted] voice services for connectivity, resilience, and capacity. MetTel's TFS will be provided for dedicated and switched terminating access arrangements. Toll Free Service connects to and interoperate with the PSTN including both wireline and wireless. TFS is provided for dedicated and switched terminating access arrangements. Our flexible TFS connectivity options will provide GSA and Agencies with scalable and resilient service.

2.1.18.5 Technical Capabilities [L.29.2.1, C.2.2.3.1.4]

MetTel offers several technical capabilities to meet all Agency TFS requirements. These capabilities support administration of toll free numbers and facilitate toll free users' interaction and communication within the Agency and with recipients of the Agency services. Our technical capabilities will ensure the Agency's current capabilities are met to avoid mission impact. MetTel's TFS solution meets all capability requirements specified in EIS Section C.2.2.3.1.4.

Exhibit 2.1.18-3: MetTel's TFS Meets All EIS Section C.2.2.3.1.4 Requirements

ID	TFS Technical Capability Provided	[redacted]
1	Serve as the responsible organization for assignment and maintenance of toll-free numbers if requested by the Agency	
2	Support and provide toll free number portability	
3	Support the Agency's currently assigned toll free numbers	
4	Provides Universal International Toll-Free Number service (UIFN) to enable the Agency request a single, unique toll-free number that is the same throughout the world (where available commercially from	

ID	TFS Technical Capability Provided
	participating countries)
5	Terminate a single toll-free number multiple locations (SDPs) and multiple toll-free numbers to terminate at a single location (SDP) as needed
6	Provide, as a default configuration, a busy signal or recorded announcement for all calls that encounter network congestion and/or terminating egress congestion, as determined by the Agency
7	Provide a network intercept to record announcements for at least 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	Provide the capability for customized network intercept recorded announcements; options for customization include: recorded by MetTel or recorded remotely by the Agency
9	Provide the capability to have announcements recorded in English and Spanish languages with other languages as optional
10	For a TFS disconnect order, Agency will be provided the option for a referral telephone number to be provided in an announcement message to callers of the disconnected toll-free number
11	Provide Dialed Number Identification Service (DNIS) to enable multiple toll-free numbers to be routed and uniquely identified on a shared trunk group; DNIS digits will be transmitted prior to delivery of a TFS call to uniquely identify the dialed toll-free number; DNIS digit length shall range from 3 to a maximum of 10 digits
12	Identify and provide the calling parties Automatic Number Identification (ANI) to assist the Agency with identifying malicious or emergency calls

2.1.18.6 Features [L.29.2.1, C.2.2.3.2]

MetTel's TFS provides several capabilities that enable and support the complete set of feature requirements in EIS Section C.2.2.3.2 and Agency's unique requirements as show in Exhibit 2.1.18-4.

Exhibit 2.1.18-4: MetTel's TFS Meets all Feature Requirements of EIS Section C.2.2.3.2

ID	Features
1	Agency Based Routing database (also known as Host Connect)

ID	Features
2	Alternate Routing (also known as "Cascade" routing)
3	ANI
4	ANI Based Routing
5	Announced Connect
6	Announcements
7	Menu Routing
8	Call Redirection

[redacted]

ID	Features
9	Computer Telephony Integration (CTI)
10	Custom Call Records
11	Day of Week Routing
12	Day of Year Routing
13	In Route Announcements
14	Interactive Voice Response (IVR)

[redacted]

ID	Features
15	Make Busy
16	Network Call Distributor

[redacted]

ID	Features
17	Network Queuing (optional)
18	NPA/NXX Routing
19	Percentage Call Allocation
20	Real Time Reporting

[redacted]

ID	Features
21	Routing Control
22	Service Assurance Routing
23	Speech Recognition
24	Tailored Call Coverage
25	Time of Day Routing
26	Language Interpretation Service
27	Virtual Queue
28	Vanity Toll Free Number

[redacted]

2.2.18.6.1 TFS Feature Reports [C.2.2.3.2.1]

At the request of the ordering Agency MetTel provides 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 capture this information on an hourly, daily, weekly, monthly, and quarterly basis. Reports contain information summarized in 30- and 60-minute increments. Multiple report formats that further summarize the information by time zone or ordering Agency region will be made available where applicable. Reports will be archived and available for a minimum of 90 days.

Reports are made available by electronic means such as a web site, or via e-mail or other MetTel-proposed applications and have the capability to export data, in a standard file format, to agency applications (e.g., spreadsheets, databases) for analysis. Reports will be made available electronically within 30 minutes of the submitted request. MetTel will 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 will 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 will 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, and (5) Toll free number(s) included in the Report

MetTel supports the TFS reporting features as detailed in **Exhibit 2.1.18-5**.

Exhibit 2.1.18-5. MetTel's Support for TFS Reporting Features

ID	Feature	[redacted]
1	Call Status Report – Toll Free Service	

ID	Feature	[redacted]
2	Call Status Report – Alternate Routing	
3	Call Status Report – Announcement	
4	Call Status Report – Call Prompter	
5	Call Status Report - IVR	

ID	Feature
6	Caller Information Report
7	Caller Profile Report

[redacted]

2.1.18.7 Interfaces [L.29.2.1, C.2.2.3.3]

Supporting a variety of interfaces provides the Agency with the ability to scale, use existing legacy infrastructure components, and equipment as needed. MetTel's TFS

supports this flexibility by meeting [redacted]

[redacted]

Exhibit 2.1.18-6. Interfaces supported by MetTel's TFS

[redacted]

[redacted]

2.1.18.8 Performance Metrics [L.29.2.1, C.2.2.3.4]

[redacted]

Our TFS meets the complete set of performance requirements (see **Exhibit 2.1.18-7**).

Exhibit 2.1.18-7. MetTel's TFS Meets the Complete Set of Performance Requirements of EIS Section C.2.2.3.4

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)
Availability (POP-to-POP)	Routine	99.95%	≥ 99.95%
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
	Critical	0.01	≤ 0.01
Time To Restore	Without Dispatch	4 hours	≤ 4 hours
	With Dispatch	8 hours	≤ 8 hours

2.1.19 Circuit Switched Data Service (CSDS) [C.2.2.4]

2.1.19.1 Compliance with Evaluation Criteria [L.29.2.1]

MetTel proposes a Circuit Switched Data Service (CSDS) solution that meets the mandatory service requirements for CSDS in C.2.2.4. This section presents a technical description of our offering, demonstrating our capabilities in Standards, Connectivity, Technical Capabilities, Features, Performance Metrics, and Interfaces. **Exhibit 2.1.19-1** highlights some key strengths and benefits of our CSDS solution in relation to RFP Section M.2.1 evaluation criteria.

Exhibit 2.1.19-1. Features and Benefits of Approach to TFS

[redacted]

2.1.19.2 Service and Functional Description [L.29.2.1, C.2.2.4.1, C.2.2.4.1.1]

MetTel's CSDS provides synchronous, full duplex, digital data transmission rates up to DS1, including integral multiples of DS0 data rates (i.e., NxDS0, where N = 1 to 24) to on-net and off-net locations. Data rates below DS1 are available in multiples of DS0 data rates. Typically, CSDS is used to support high-bandwidth services such as on-demand video conferencing.

2.1.19.3 Standards [L.29.2.1, C.2.2.4.1.2]

Our CSDS complies with the following standards: [redacted]

[redacted] Our engineering staff maintains awareness of all new versions, amendments, and modifications to the standards list above. We regularly meet with hardware and software vendors to discuss their product roadmaps to understand new and planned features and capabilities are impacted by changing standards. This helps us address technology and product obsolescence and ensure we take advantage of technologies as they are fielded. This results in providing Agencies with up-to-date CSDS.

2.1.19.4 Connectivity [L.29.2.1, C.2.2.4.1.3]

MetTel's CSDS connectivity is flexible and will support connections to and interoperates with a host of networks. Specifically, we designed our CSDS to connect to and interoperate with:

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

2.1.19.5 Technical Capabilities [L.29.2.1, C.2.2.4.1.4]

Our CSDS solution provides all eight mandatory technical capabilities required by EIS Section 2.2.4.1.4, as referred to in Exhibit 2.1.19-2.

Exhibit 2.1.

Requirement	[redacted]
1. Uniform Numbering Plan	
2. Authorization Codes for CSDS	
3. Calls Terminating to Off-Net Locations	
4. Scheduling Calling Capability	
5. Clocking	

Requirement	[redacted]
6. Bit Sequence Integrity	
7. Dialable Bandwidth	
8. Multirate DS0	

We follow industry's technology trends and capabilities to ensure the highest level of technical capabilities to our customers. We follow technology insertion roadmaps for each of our services to ensure they are current and that ***technologies and products are not obsolete***. As products reach end-of-life, we develop plans to replace those products with up-to-date components.

2.1.19.6 Features [L.29.2.1, C.2.2.4.2]

[redacted]

Access to CSDS is only provided after verification of the authorization code entered by the users. Authorization codes provide management reporting benefits and are verified in our secure, intelligent network database to determine whether the caller has authorization to access CSDS. [redacted]

2.1.19.7 Interfaces [L.29.2.1, C.2.2.4.3]

[redacted] We regularly upgrade our components to field new technologies and capabilities.

Exhibit 2.1.19-3: MetTel's Interface Options Provide SSA with Flexibility for CSDS

[redacted]

2.1.19.8 Performance Metrics [L.29.2.1, C.2.2.4.4]

MetTel designed our CSDS solution to be redundant, highly available, responsive, and provide scalable capacity. [redacted]

Exhibit 2.1.19-4: Performance Metrics for MetTel's CSDS Solution

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)
Availability (POP-to-POP)	Routine	99.95%	≥ 99.95%

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)
Availability (SDP-to-SDP)	Routine	99.5%	> 99.5%
	Critical	99.95%	> 99.95%
Time to Restore	With Dispatch	8 hours	≤ 8 hours
	Without Dispatch	4 hours	≤ 4 hours
Grade of Service (Call Blockage)	Routine	0.07 (SDP-to-SDP)	<0.07
		0.01 (POP-to-POP)	< 0.01
	Critical	0.01 (SDP-to-SDP & POP-to-POP)	< 0.01

[redacted] We will provide Agency approved users with accounts and access to performance information. [redacted] we will review and report on performance metrics during monthly program meetings.

2.1.20 Audio Conferencing Service [C.2.8.7]

2.1.20.1 Compliance with Evaluation Criteria [L.29.2.1]

MetTel proposes an Audio Conferencing Service (ACS) solution that meets the mandatory service requirements for ACS in C.2.8.7. This section presents a technical description of our offering, demonstrating our capabilities in Standards, Connectivity, Technical Capabilities, Features, Performance Metrics, and Interfaces. **Exhibit 2.1.20-1** highlights some key strengths and benefits of our ACS solution in relation to RFP Section M.2.1 evaluation criteria.

Exhibit 2.1.20-1. Features and Benefits of Approach to TFS

[redacted]

[redacted]

2.1.20.2 Service and Functional Description [L.29.2.1, C.2.8.7.1, C.2.8.7.1.1]

MetTel's ACS provides a reliable high-quality audio conferencing service that enables agencies to collaborate with colleagues in a multi-point audio conferencing call. Workers in the office, at home or on the go, can utilize MetTel's ACS mobile and desktop apps to start meetings faster by connecting without dialing numbers or passcodes. [redacted]

2.1.20.3 Standards [L.29.2.1, C.2.8.7.1.2]

Adherence to industry and government ACS standards ensures the Agency has a secure, reliable, flexible, scalable, and resilient service. Our voice engineers and product managers monitor changes to standards to determine the impact to our ACS and implement upgrades when feasible. This ensures our ACS continues to provide features and benefits brought and avoids technology obsolescence. MetTel's ACS complies with the standards seen in **Exhibit 2.1.20-2**.

[redacted]

[redacted]

2.1.20.4 Connectivity [L.29.2.1, C.2.8.7.1.3]

MetTel's ACS provides the Agency users multiple connectivity options from anywhere in the world and allows users to interconnect in a variety of ways such as through the PSTN or connect via Internet-based calling. Our ACS service connects through MetTel's CSVS or IPVS and therefore enjoys the redundancy and performance of those services. Our ACS is fully compatible with and operates over any other service providers CSVS or IPVS. This results in the Agency's ability to use our ACS anytime and under any condition. MetTel's Audio Conferencing Service will connect to and interoperate with:

- Customer-specified locations
- PSTN
- Internet
- MetTel's network and all other contractors' networks for Circuit Switched Voice Service and IP Voice Service.

2.1.20.5 Technical Capabilities [L.29.2.1, C.2.8.7.1.4]

Exhibit 2.1.20-3 shows the EIS Section C.2.8.7.1.4 capabilities that our solution provides.

Exhibit 2.1.20-3: MetTel's Audio Conferencing Service Technical Capability

MetTel ACS Capability	[redacted]
Selective two-way or one-way conversations between conferencing ports	
Addition of a party to, or the deletion of a party from, the conference is indicated by	

MetTel ACS Capability	[redacted]
a tone or verbal announcement	
User-Controlled Conference	
Meet-Me Conference	
Preset Conference	
Attendant-Assisted Conference	
Audio Conference Reservation System	
Automatic port expansion	
Conferee tones	
Participant count	

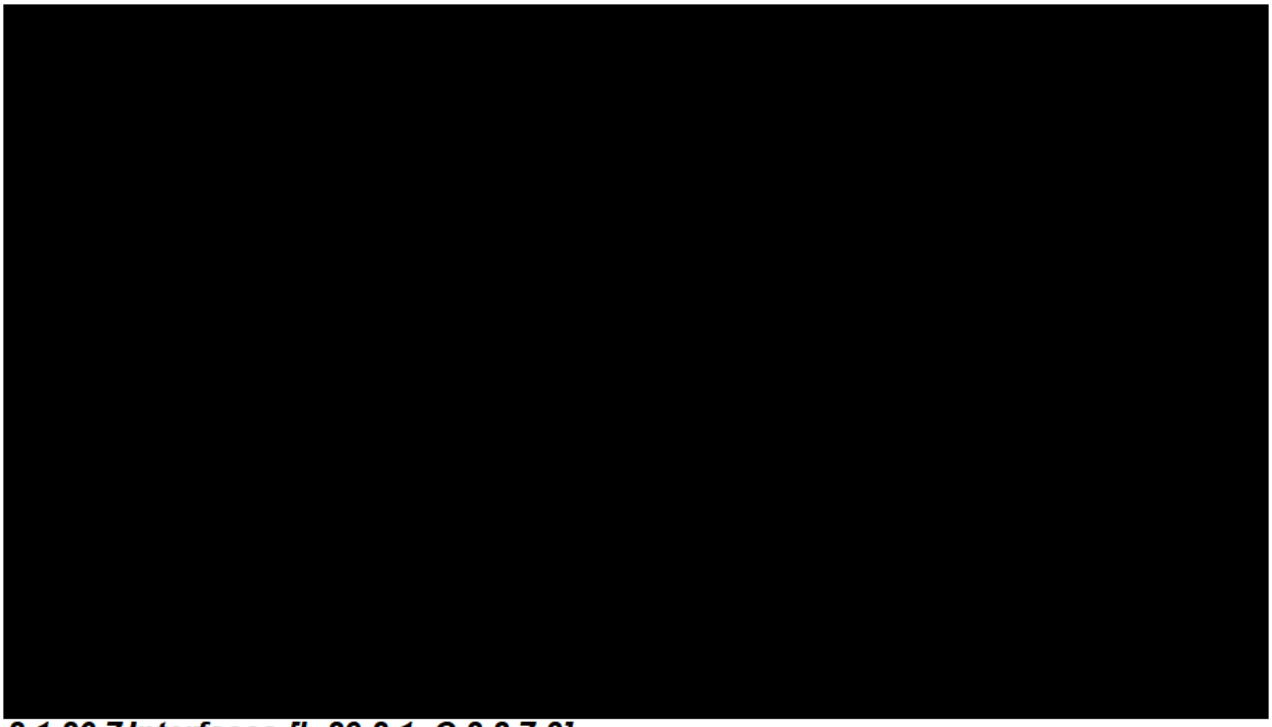
MetTel ACS Capability	[redacted]
Roll call	
Attendant assistance	

2.1.20.6 Features [L.29.2.1, C.2.8.7.2]

MetTel's ACS solution provides the features shown in Exhibit 2.1.20-4.

Exhibit 2.1.20-4: Features of MetTel's ACS Solution

[redacted]



2.1.20.7 Interfaces [L.29.2.1, C.2.8.7.3]

MetTel's ACS supports audio connection to the conference bridge from Voice Services and Cellular Voice services. Conference call hosts can dial designate numbers to initiate conference services from any type of Voice Service platform, Circuit switched or Voice over IP (VoIP) services.

2.1.20.8 Performance Metrics [L.29.2.1, C.2.8.7.4]

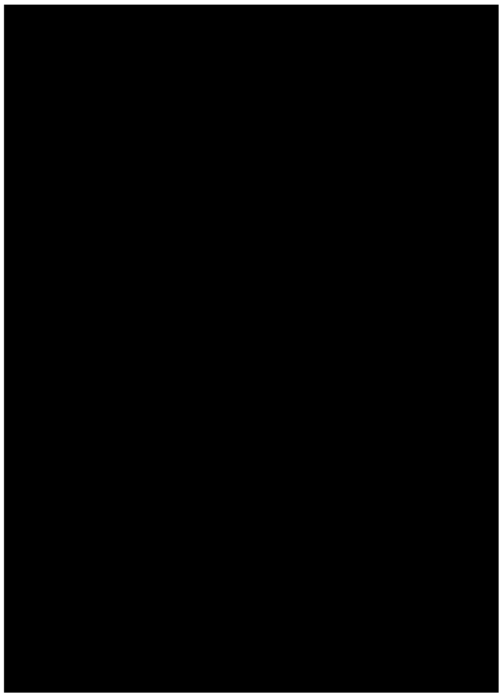
Performance metrics, measurement, and reporting ensures ACS is reliable, resilient, and provides high quality voice transmission for the Agency. MetTel's ACS meets the performance levels and Acceptable Quality Level (AQL) of Key Performance Indicators (KPIs) for Audio Conferencing Service as described EIS Section C.2.8.7.4 and as reflected in Exhibit 2.1.20-5.

Exhibit 2.1.20-5: Performance Metrics for MetTel's ACS Solution

KPI	Service Level	Performance Standard (Threshold)	AQL
Availability	Routine	99.5%	≥ 99.5%
GOS (Operator Assistance Response Delay)	Routine	30 seconds	≤ 30 seconds
Time to Restore	With Dispatch	8 hours	≤ 8 hours
	Without Dispatch	4 hours	≤ 4 hours

[redacted]

2.1.21 Private Line Service (PLS) [C.2.1.4]



MetTel's PLS provides Agencies with dedicated circuits, private switching arrangements, and/or predefined transmission paths, whether virtual or physical, which provide communications between specific locations. MetTel's PLS can connect two locations, if needed, but may also be switched at either end or both ends for additional flexibility and connectivity options.

2.1.21.1 Compliance with Evaluation Criteria [L.29.2.1]

We have multiple carrier partner providers in most CBSAs and use this competitive edge to offer the most cost-effective, reliable solutions for Agencies. We have wholesale partnerships with most of the Local Exchange Carriers (LECs), Tier-1 carriers and ISPs, and cable and wireless providers. Through these partnerships, we provide the right PLS technology complete with customized access, required diversity, and path avoidance. With this approach, we have eliminated the constraints of a single provider, single access provider, or single hardware vendor. We have the freedom to select the most cost-effective, best PLS solution, based on scalability, reliability, resilience, flexibility, and security requirements. Exhibit 2.1.21-1 summarizes our PLS solution against the evaluation criteria.

Exhibit 2.1.21-1. MetTel's Complies with all PLS Evaluation Criteria and Requirements

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• Agencies can use MetTel's PLS to meet a diverse set of operational requirements for telecommunications connectivity • Agencies can manage their dedicated PLS connections which are committed to a single Agency • MetTel's PLS supports multiple protocols allowing Agencies to transmit voice, data, video, and multi-media • MetTel's PLS can be encrypted using an Agencies own encryption

Evaluation Criteria	Features and Benefits of MetTel's Approach
	approaches to enhance a security
Quality of Services (M.2.1(2))	• MetTel's PLS is a standards-based service that meets all mandatory connectivity, technical capabilities, and features over a wide range of interface capabilities; results in high performing and high-quality service
Service Coverage (M.2.1(3))	• MetTel meets the minimum CBSA requirements

Security (M.2.1(4a)	• MetTel implements basic and best practice security protocols for all services, including PLS. This includes the following within the confines of requirements, Agency responsibilities, and Agency approvals.
	  • Equipping physical buildings and rooms with backup power and HVAC capabilities with the ability to operate for some time without interruption
	  • Providing lockable cabinet spaces as required
	  • Ensuring only authorized personnel have access to physical locations of PLS components' locations
	  • Providing in-service remote monitoring and environmental monitoring to the maximum extent possible

Security [M.2.1(4b; C.1.8.7]	• MetTel's Risk Management Framework Plan describes our approach for security compliance for all services provided under EIS • MetTel provides basic physical and logical protection of services, information, MetTel infrastructure, and information processing resources against threats, attacks, or system failures • MetTel performs extensive engineering review, evaluation, and testing to ensure our PLS complies with all Federal Information Security Management Act (FISMA), DOD, and Intelligence Community requirements where applicable in specific TOs
Security [M.2.1(4c); C.1.8.8]	• Refer to Section 2.3 External Traffic Routing Requirement of MetTel's EIS proposal for a thorough description of MetTel's solution for external traffic routing
Security (M.2.1(4d)	• MetTel's Risk Management Framework Plan (see Attachment 1) describes our approach for security compliance for all services provided under EIS

2.1.21.2 Service and Functional Description [L.29.2.1 C.2.1.4.1, C.2.1.4.1.1]

MetTel's redundant networks, components, and facilities help ensure that our PLS provides Agencies with reliable full-duplex transmission and connectivity options. Further, this allows us to offer connectivity between dedicated end-points with options for additional drops. This level of diversity and design flexibility supports multiple types of transmission applications including voice, data, video, multi-media, and encryption of connectivity if needed. Our PLS's enhanced technical capabilities (shown in Exhibit 2.1.21-3 and Exhibit 2.1.21-4) meet a wide range of bandwidth, speed, and technical characteristics for any Agency.Exhibit 2.1.21-3. General Technical Capabilities of MetTel's PLS

2.1.21.3 Standards [L.29.2.1 C.2.1.4.2]

Adherence to industry and government PLS standards ensures Agencies have a secure, reliable, flexible, scalable, and resilient service that results in consistent performance, and reduces technology transition risks. MetTel's PLS engineers and product managers monitor changes to standards to determine the impact to our PLS and implement upgrades when feasible. This results in providing Agencies with features and benefits brought about by new technology advancements and avoids technology obsolescence. MetTel's PLS complies with the standards seen in Exhibit 2.1.21-2.

Exhibit 2.1.21-2. MetTel's PLS Adheres to the Full Range of Industry Standards

MetTel PLS Standards Compliance	Benefit for Agency
ANSI T1.102/107/401/403/503/510 for T1	MetTel's PLS supports this standard
Telcordia PUB GR-499-CORE for T3	MetTel's PLS supports this standard
ANSI T1.105 and 106 for SONET	MetTel's PLS supports this standard
Telcordia PUB GR-253-CORE for SONET	MetTel's PLS supports this standard
ITU-TSS G.702 and related Recommendations for E1 and E3	MetTel's PLS supports this standard
Telcordia PUB SR-TSV-002275, TR-NWT-000965, and TR-NWT-000335 for analog	MetTel's PLS supports this standard
Telcordia PUB GR-418-CORE for reliability/performance	MetTel's PLS supports this standard

2.1.21.4 Connectivity [L.29.2.1 C.2.1.4.1.3]

With an extensive U.S. domestic network infrastructure, MetTel connects Agencies to one of the most advanced networks in the country and interfaces with other EIS contractors as needed. As a result, Agencies will have cost-effective PLS that supports various applications such as voice, data, video, multimedia, and encrypted

communications. Our PLS extends the reach of Agencies' internal communications infrastructure by terminating with SDPs such as PBXs, Multiplexers, Routers, Video CODECs, and Group 4 FAXs. MetTel's private lines provide point-to-point digital data connectivity (not part of the public switched network) which can link multiple Agency sites to each other or to network nodes with a fully managed high-speed service. Connectivity between end points is permanent unless and until modified at Agency request.

2.1.21.5 Technical Capabilities [L.29.2.1 C.2.1.4.1.4]

MetTel's PLS meets all general technical capabilities as shown in Exhibit 2.1.21-3.

Exhibit 2.1.21-3. General Technical Capabilities of MetTel's PLS

MetTel PLS General Technical Capabilities	[redacted]
Routing requirements in Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection	
Transparency to any protocol	
Data transparency treatment of all bit sequences transmitted by GFP through the SDP	

MetTel's PLS offers support to a wide range of standards-based data rates. Support for this technical capability provides Agencies with a flexible and scalable service to meet an array of diverse mission requirements. See Exhibit 2.1.21-4 for the data rates supported by MetTel.

Exhibit 2.1.21-4. MetTel's PLS Supports the Full Range of Data Rate Categories

Item	MetTel PLS Data Rate Technical Capabilities	[redacted]
1	DS0	
2	T1	
3	T3	
4	E1	
5	E3	
6	(Optional) SONET OC-1	

7	(Optional) SONET OC-1; Virtual Tributary	[redacted]
8	SONET OC-3	
9	SONET OC-12	
10	SONET OC-48	
11	SONET OC-192	
12	(Optional) SONET OC-768	
13	(Optional) Subrate DS0	
14	(Optional) Analog Line (4KHz)	
15	(Optional) Fractional T1	
16	Fractional T3	

2.1.21.6 Features [L.29.2.1 C.2.1.4.2]

MetTel's PLS meets all feature requirements shown in Exhibit 2.1.21-5. The result is that Agencies will be supported in all mission and operational needs.

Exhibit 2.1.21-5. MetTel's PLS Meets All Feature Requirements

Name of Feature	[redacted]
Branch-Off	
Drop-and-Insert	
Transport Diversity	
Transport Avoidance	

2.1.21.7 Interfaces [L.29.2.1 C.2.1.4.3]

Supporting a variety of interfaces provides Agencies with the ability to maximize PLS options and use existing legacy infrastructure components and equipment as needed to ease transition to new services. MetTel's TFS supports this interface flexibility by meeting all interface requirements established and documented in EIS Section C.2.1.4.3 as shown in Exhibit 2.1.21-6.

Exhibit 2.1.21-6. MetTel's PLS Supports a Wide Range of Interface Options for Agencies

Item	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
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	SONET OC-768c (Std: ANSI T1.105 and 106)	38.486016 Gbps	Transparent

Item	Interface Type and Standard	Payload Data Rate	UNI Type
(Optional)			

2.1.21.8 Performance Metrics [L.29.2.1 C.2.1.4.4]

Adherence to standards, flexible and robust connectivity options, and key features (e.g., transport diversity and transport avoidance contribute to our ability to meet PLS performance metrics, measures, and levels. In addition, MetTel embedded automated network performance monitoring and measurement tools to collect, measure, and report on KPIs. This includes use of automated event notification capabilities to quickly notify our 24x7 network operations center of PLS outages or degradations and results in quicker troubleshooting, time-to-restore, and higher availability. These ensure we can meet the performance levels and AQL of KPIs for PLS circuits. See Exhibit 2.1.21-7.

Exhibit 2.1.21-7. Performance Metrics for MetTel's PLS Solution

Key Performance Indicator	Service Level	Performance Standard (Threshold)	Acceptable Quality Level
Availability (POP-to-POP)	Routine	99.9%	≥ 99.9%
	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
	With Dispatch	8 hours	≤ 8 hours

2.2 Information Security [L.11, L.29.2.2, J.14]

MetTel Information Security

[redacted]

MetTel's approach to completing the security plan and certification and security authorization is included in Attachment 1, Risk Management Framework Plan. The Plan also addresses how we ensure the delivery of system security for the EIS services as specified in Section C.1.8.7.

MetTel's plan to address system security as specified in Section C.2.8.4.5 is included in Attachment 2, MTIPS Risk Management Framework Plan.

[redacted]

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.

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

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]

[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)]

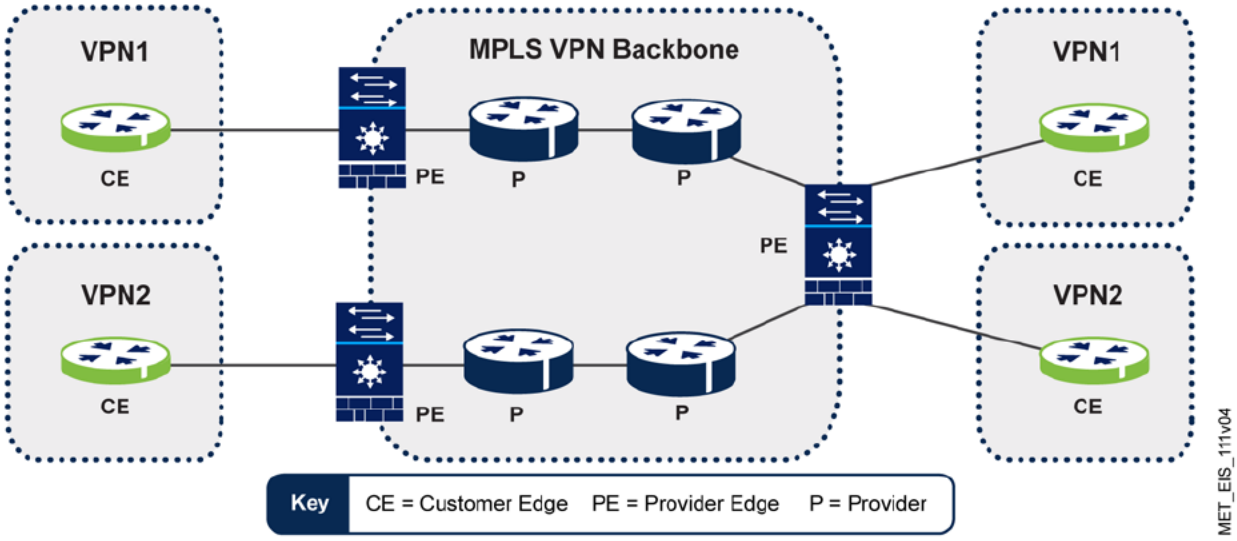
To meet the External Traffic Routing requirements, the MetTel Team will build the MTIPS Portals [redacted] for inspection prior to delivery to destination. In the event an agency has bifurcated its data network and MTIPS, the routing discussed below will still apply.

The MetTel Team routes all traffic to one of three MTIPS Portals (or to the Agency's MTIPS provider). Each Portal is configured with a Participating Agency-specific configuration for the combined security service. Internet-bound traffic reaches the Internet via the designated MTIPS Portal, with the alternative MTIPS Portal configured as High Availability (HA) backup MTIPS Portals. In the case of MetTel being the MTIPS provider, using standard BGP, traffic from the Participating Agency's CE router is routed to respective MTIPS Portals. We also accommodate load sharing based on IP address.

The BGP announces routes from the router at the Participating Agency's SDP to the [redacted] In the event [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] for the Participating Agency based on [redacted].

Our external routing solution provides defense in layers by de [redacted] At the top layer, Internet access routers provide connectivity to and from the Internet. [redacted]

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



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)

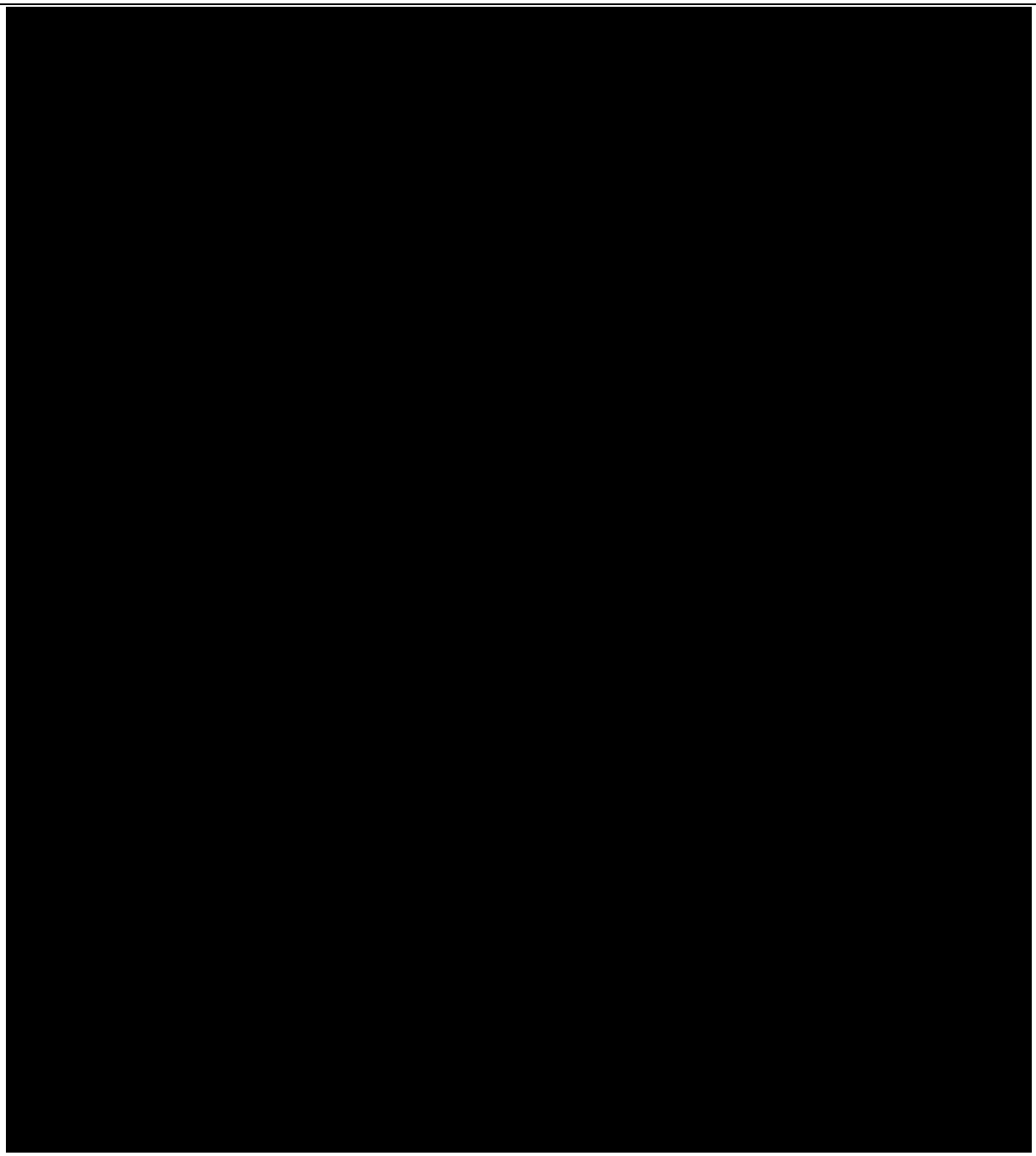
Exhibit 2.3-1. MPLS Device Roles

[redacted]

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]



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

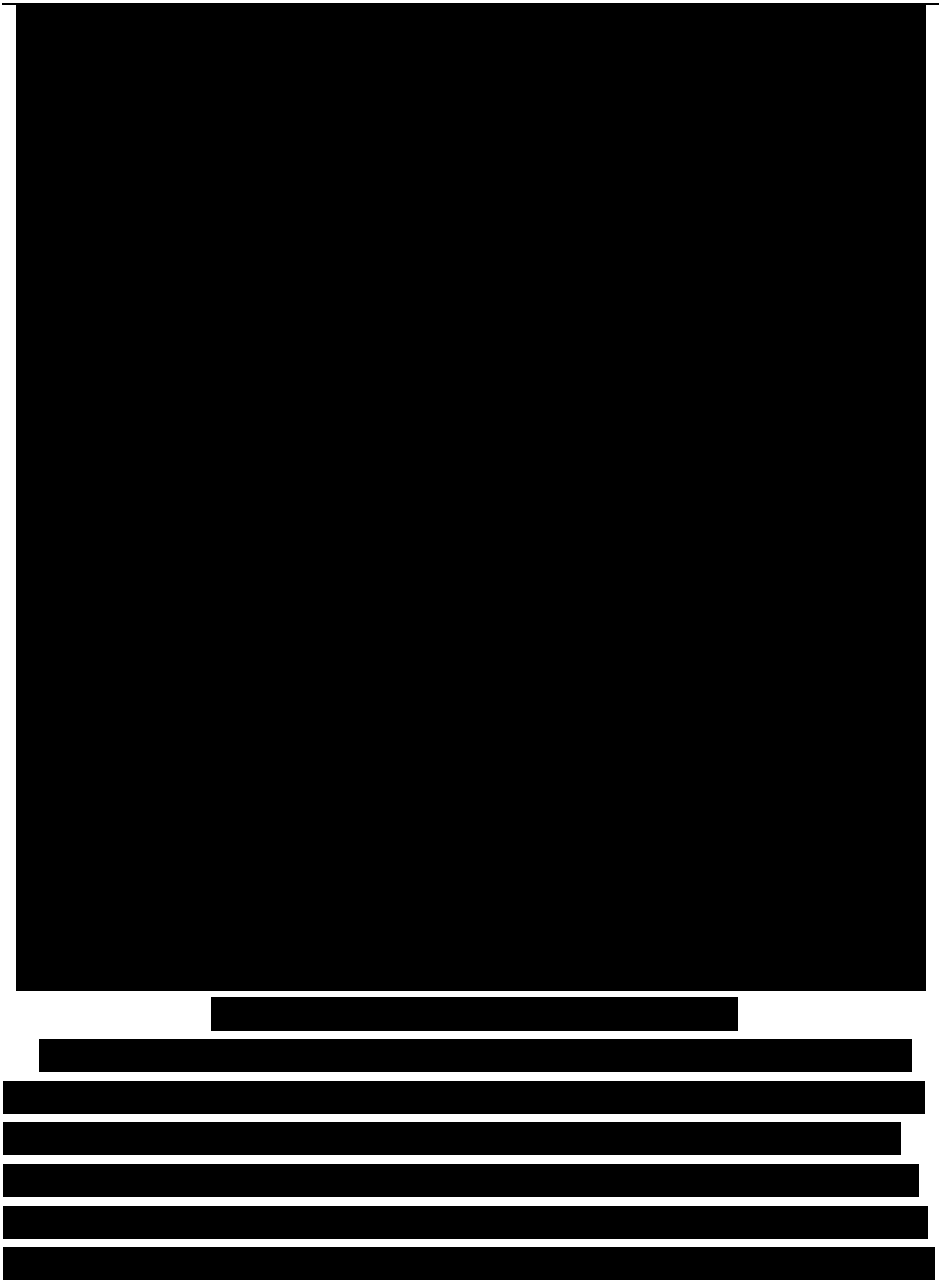
[redacted]

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]

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

[redacted] VPN access point supports dedicated external connections to external partners and business partners as well as MetTel MPLS connected Participating Agencies. [redacted] The following baseline capabilities are supported for external dedicated VPN and private line connections at the VPN Access Point:

[redacted]

[redacted]

Our Extranet access point supports dedicated Extranet connections to internal partners. [redacted]

[redacted]

[redacted]

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

[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] Agencies benefit from high-quality services derived from a stable, proven network platform. [redacted]

[redacted] service enables aggregation and flexibility in accessing the MTIPS gateway. Our architecture also provides diverse route and POP access to the MetTel [redacted] network, eliminating single points-of-failure between a Participating Agency's location and the MetTel MTIPS gateway. Our architecture ensures that all Agency traffic continues to flow and remains secure even if the Internet becomes unavailable due to an attack.

Once an alert is triggered, we notify the Participating Agency. Relevant data is stored and accessible by the Participating Agency via appropriately classified and approved communication channels. In the event of component or capability degradation or failure, the system's health data is likewise transmitted to DHS and Participating Agencies. System event tracking records all activity concerning the operations and management of our [redacted] and MTIPS Enclave. [redacted]

2.3.4 Control Mechanisms to Ensure No By-Pass [L.29.2.3 (4)]

[redacted]

2.3.5 Sensing and Control Mechanisms to Ensure Traffic Failsafe [L.29.2.3 (5)]

Central to the External Traffic Routing design is [redacted]

[redacted]

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

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

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

3.0 SATISFACTION OF 508 REQUIREMENTS [C.4, F.2.1(33)]

MetTel's approach to meeting Section 508 criteria for the services identified in C.4.4 of the EIS RFP includes a range of activities to ensure that all users are able to access all MetTel-proposed EIS services.

MetTel's Service Availability and 508 Compliance is Central to our Service Delivery

- 508 compliance begins at the design phase of our service development
- Our commitment to making our services available to all users is ensured by building our MetTel's EIS Portal, based on our award-winning commercial platform, Bruin.
- Testing for compliance and VPAT submissions are kept current by our 508 Project Manager, [redacted]

MetTel achieves compliance by performing the same testing and evaluation process that all products and services go through before they are released commercially. MetTel works with our preferred providers to ensure that our services satisfy the Section 508 requirements. MetTel tests with and evaluates industry specific Associative Technology (AT) vendors to assess interoperability with TeleTYpewriter (TTY) and AT devices. The MetTel services offered for EIS are identified in **Exhibit 3-1** with the associated Section 508 requirements that apply.

Exhibit 3-1. Section 508 Requirements for MetTel EIS Services.

[redacted]

MetTel has a toll-free number (1-877-2Go-2EIS) which provides Agencies with direct access to MetTel Customer Support. This number is 508 compliant, enabling access by Email (EIS@MetTel.net), FAX, TTY, telecommunications display devices, text messaging, or other methods as required. In addition, the MetTel EIS portal is 508 compliant so that EIS service users can access all the information and capabilities in a 508 compliant manner.

The following describes the MetTel approach for maintaining compliance with Section 508. The MetTel approach for 508 compliance includes working with the service providers and device manufacturers that MetTel relies on to deliver the EIS offerings. The following are the major components of the MetTel 508 compliance program.

Discovery and Scoping

MetTel will provide the Voluntary Product Accessibility Templates (VPATs) developed for each offered service not later than 30 days after authorization to proceed. The VPATs will address the requirements for the services defined in **Exhibit 3-1** and evaluated against the following requirements:

- 1194.21 Software Application and Operating System
- 1194.22 Web Based Internet Information and Applications
- 1194.23 Telecommunications Products
- 1194.31 Functional Performance Criteria
- 1194.41 Information, Documentation, and Support

This evaluation will identify and resolve compliance issues in existing requirements or services. This information will also be used to develop future releases of MetTel services to ensure compliance with Section 508 for future enhancements and releases.

MetTel Section 508 Project Manager (PM), [redacted], is responsible for the testing and integration of products and services with Assistive Technologies. The PM works with SRE manufactures and service providers to ensure that Section 508 compliance is an integral part of the design process for all new and future hardware and software releases.

The Section 508 PM reports to the MetTel Program Manager every month providing any updated VPATs and Technical Reports as required by Section C.4.5 of the EIS RFP and delivered to the GSA EIS Program Management Office (PMO).

Design Guidelines

MetTel focuses on developing accessibility design guidelines for use and reference by our internal software development teams, MetTel consultants, and preferred providers. The guidelines will be updated as tools are identified for developers and implementers to use in the design, development, and testing of the business applications. MetTel will use these guidelines in discussions with providers and developers to ensure that the MetTel services for EIS will maintain compliance with Section 508. These guidelines will be reviewed and updated at least monthly and will be addressed as part of each project's monthly review with the EIS PMO.

Training

Training may be delivered via meetings and briefings, classrooms, seminars, instructor-led and non-instructor online Web-based self-study, and through manuals or desktop guides. For training delivered via meetings, briefings, classrooms, and seminars, assistance such as signers and Braille products will be provided to disabled trainees when requested in advance by the Agency involved. For training delivered via instructor-led and non-instructor online Web-based study, the same capabilities provided for Internet reporting shall be provided to disabled trainees. For self-study and manuals or desktop guides using audio/video tapes, CD-ROM, or DVD, MetTel will comply with the relevant provisions as shown in **Exhibit 3-1**.

[redacted]

The MetTel PM will be responsible for managing the development of MetTel-offered EIS service training, documentation, manuals, user guides, audio/visual tapes, CD ROMS, and DVDs for disabled users as defined in Agency Task Orders (TO).

[redacted]

[redacted]

MetTel will continue to work with service providers and vendors to explore ways to participated in programs focused on accessibility and Section 508 compliance.

Subpart C, Functional Performance Criteria

MetTel is committed to providing services that meet the needs of disabled employees and citizens' AT. Agencies may have a variety of disabled users, accessing a variety of systems, equipment, and applications using a variety of EIS services. MetTel seeks to ensure that disabled users are satisfied with our service offerings. MetTel has identified the following as key principles in meeting the needs of disabled users of MetTel services.

- Support specific Agency requirements for users
- Provide equivalent access to auditory and visual content based on specific Agency requirements
- Provide interoperability and compatibility with AT and include complete keyboard access when applicable
- Provide context and system orientation when and where needed
- Follow Section 508 specifications and guidelines to ensure compliance and confirm services meet requirements.