



EIS
Enterprise Infrastructure Solutions (EIS)
NS2020

Volume 1 - Technical Proposal

Solicitation No.: QTA0015THA3003

Date: November 4, 2016

Submitted to: General Services Administration FAS/ITS

Submitted by: Core Technologies, Inc.

Table of Contents

Table of Contents

1.0	NETWORK ARCHITECTURE (L.29.1) [RIN: MTR0102-DN]	1
1.1	UNDERSTANDING	1
1.2	QUALITY OF SERVICES	7
1.3	SERVICE COVERAGE [RIN: MTR2249-KS]	7
1.4	SECURITY [RIN: MTR0114-DN]	8
2.0	TECHNICAL RESPONSE (L.29.2)	16
2.1	EIS SERVICES (L.29.2.1) [RIN: MTC0013-DI]	16
2.1.1	EIS Scope for Mandatory Services (C.1.2)	16
2.1.1.1 Data Services (C.2.1).....	16
2.1.1.1.1	VIRTUAL PRIVATE NETWORK SERVICE (C.2.1.1) [RIN: MTR0131-DN].....	16
2.1.1.1.1.1	... <i>Service Description (C.2.1.1.1)</i>	16
2.1.1.1.1.1.1 Functional Definition (C.2.1.1.1.1).....	17
2.1.1.1.1.1.2 Standards (C.2.1.1.1.2) [RIN: MTC0002-DI]	19
2.1.1.1.1.1.3 Connectivity (C.2.1.1.1.3)	21
2.1.1.1.1.1.4 Technical Capabilities (C.2.1.1.1.4) [RIN: MTR0010-DN]	21
2.1.1.1.1.2	... <i>Features (C.2.1.1.2)</i>	24
2.1.1.1.1.3	... <i>Interfaces (C.2.1.1.3) [RIN: MTR0106-DN, MTR0005-DN]</i>	25
2.1.1.1.1.4	... <i>Performance Metrics (C.2.1.1.4) [RIN: MTR0006-DN]</i>	25
2.1.1.1.2	ETHERNET TRANSPORT SERVICE (C.2.1.2).....	26
2.1.1.1.2.1	... <i>Service Description (C.2.1.2.1)</i>	26
2.1.1.1.2.1.1 Functional Definition (C.2.1.2.1.1).....	28
2.1.1.1.2.1.2 Standards (C.2.1.2.1.2).....	29
2.1.1.1.2.1.3 Connectivity (C.2.1.2.1.3)	31
2.1.1.1.2.1.4 Technical Capabilities (C.2.1.2.1.4) [RIN: MTR0113-DN, MTR2244-DN, MTC0003-DI]	31
2.1.1.1.2.2	... <i>Features (C.2.1.2.2) [RIN: MTR0069-DN]</i>	37
2.1.1.1.2.4	... <i>Performance Metrics (C.2.1.2.4) [RIN: MTC0005-DI]</i>	39
2.1.1.2 Voice Service (C.2.2)	41

2.1.1.2.1	INTERNET PROTOCOL VOICE SERVICE (C.2.2.1).....	42
2.1.1.2.1.1	... <i>Service Description (C.2.2.1.1) [RIN: MTC0014-DI]</i>	42
2.1.1.2.1.1.1 Functional Definition (C.2.2.1.1.1) [RIN: MTR0027-DN].....	44
2.1.1.2.1.1.2 Standards (C.2.2.1.1.2) [RIN: MTR0020-DN].....	45
2.1.1.2.1.1.3 Connectivity (C.2.2.1.1.3)	45
2.1.1.2.1.1.4 Technical Capabilities (C.2.2.1.1.4) [RIN: MTR0028-DN]	46
2.1.1.2.1.2	... <i>Features (C.2.2.1.2)</i>	49
2.1.1.2.1.3	... <i>Interfaces (C.2.2.1.3)</i>	51
2.1.1.2.1.4	... <i>Performance Metrics (C.2.2.1.4)</i>	51
2.1.1.2.1.5	... <i>Managed LAN Service (C.2.2.1.5)</i>	52
2.1.1.2.1.6	... <i>Session Initiating Protocol Trunk Service (C.2.2.1.6)</i>	54
2.1.1.2.1.6.1 Technical Capabilities (C.2.2.1.6.1)	54
2.1.1.2.1.6.2 Features (C.2.2.1.6.2).....	54
2.1.1.3 Managed Network Services (C.2.8.1).....	54
2.1.1.3.1	SERVICE DESCRIPTION (C.2.8.1.1) [RIN: MTR0129-DN]	54
2.1.1.3.1.1	... <i>Functional Definition (C.2.8.1.1.1)</i>	56
2.1.1.3.1.2	... <i>Standards (C.2.8.1.1.2)</i>	57
2.1.1.3.1.3	... <i>Connectivity (C.2.8.1.1.3)</i>	57
2.1.1.3.1.4	... <i>Technical Capabilities (C.2.8.1.1.4)</i>	58
2.1.1.3.1.4.1 Design and Engineering Services (C.2.8.1.1.4.1) [RIN: MTR0031-DN, MTR0110-DN, MTR0111-DN, MTR0120-DN, MTR0115-DN, MTR0116-DN, MTR0117-DN, MTR0118-DN, MTR0119-DN].....	58
2.1.1.3.1.4.2 Implementation, Management and Maintenance (C.2.8.1.1.4.2).....	62
2.1.1.3.2	FEATURES (C.2.8.1.2) [RIN: MTR0054-DN].....	67
2.1.1.3.3	INTERFACES (C.2.8.1.3).....	69
2.1.1.3.4	PERFORMANCE METRICS (C.2.8.1.4) [RIN: MTR0053-DN]	69
2.1.1.4 Access Arrangements (C.2.9) [RIN: MTR0063-DN]	69
2.1.1.4.1	ACCESS ARRANGEMENT DESCRIPTION (C.2.9.1).....	69
2.1.1.4.1.1	... <i>Functional Definition (C.2.9.1.1)</i>	70
2.1.1.4.1.2	... <i>Standards (C.2.9.1.2)</i>	71
2.1.1.4.1.3	... <i>Connectivity (C.2.9.1.3)</i>	72

2.1.1.4.1.4... Technical Capabilities (C.2.9.1.4) [RIN: MTR2245-DN, MTR2250-DN].....	72
2.1.1.4.2 ACCESS DIVERSITY AND AVOIDANCE (C.2.9.2).....	77
2.1.1.4.3 INTERFACES (C.2.9.3) [RIN: MTR0157-DN].....	78
2.1.2 EIS Scope for Optional Services (C.1.2) [RIN: MTR0161-DN].....	79
2.1.2.1 Data Service (C.2.1)	79
2.1.2.1.1 VIRTUAL PRIVATE NETWORK SERVICE* (C.2.1.1).....	79
2.1.2.1.2 ETHERNET TRANSPORT SERVICE* (C.2.1.2).....	79
2.1.2.1.3 OPTICAL WAVELENGTH SERVICE (C.2.1.3).....	79
2.1.2.1.4 PRIVATE LINE SERVICE (PLS) (C.2.1.4).....	80
2.1.2.1.5 SYNCHRONOUS OPTICAL NETWORK SERVICES (SONET) (C.2.1.5)	80
2.1.2.1.6 DARK FIBER SERVICES (DFS) (C.2.1.6)	80
2.1.2.1.7 INTERNET PROTOCOL SERVICE (C.2.1.7).....	80
2.1.2.2 Voice Service (C.2.2)	80
2.1.2.2.1 INTERNET PROTOCOL VOICE SERVICE* (C.2.2.1).....	80
2.1.2.2.2 CIRCUIT SWITCHED VOICE SERVICE (C.2.2.2).....	80
2.1.2.2.2.1 ... Service Description (C.2.2.2.1)	80
2.1.2.2.2.1.1 Functional Definition (C.2.2.2.1.1) [RIN: MGC0001- DI, MTR2251-DN].....	81
2.1.2.2.2.1.2 Standards (C.2.2.2.1.2).....	82
2.1.2.2.2.1.3 Connectivity (C.2.2.2.1.3)	82
2.1.2.2.2.1.4 Technical Capabilities (C.2.2.2.1.4)	83
2.1.2.2.2.2 ... Features (C.2.2.2.2)	84
2.1.2.2.2.3 ... Interfaces (C.2.2.2.3).....	88
2.1.2.2.2.4 ... Performance Metrics (C.2.2.2.4)	89
2.1.2.2.3 TOLL FREE (C.2.2.3).....	90
2.1.2.2.4 CIRCUIT SWITCHED DATA SERVICE (CSDS) (C.2.2.2)	90
2.1.2.3 Contact Center Services (C.2.3).....	90
2.1.2.4 Collocated Hosting Center Services (C.2.4)	90
2.1.2.5 Cloud Services (C.2.5) [RIN: MTR0084-DN].....	90
2.1.2.5.1 INFRASTRUCTURE AS A SERVICE (C.2.5.1) [RIN: MTR0142-DN, MTR0160-DN, MTR0084-DN].....	95
2.1.2.5.1.1 ... Service Description (C.2.5.1.1) [RIN: MTR0084-DN]	96
2.1.2.5.1.1.1 Functional Definition (C.2.5.1.1.1).....	102
2.1.2.5.1.1.2 Standards (C.2.5.1.1.2) [RIN: MTR0128-DN].....	103

2.1.2.5.1.1.3	Connectivity to Cloud Data Center (C.2.5.1.1.3)	105
2.1.2.5.1.1.4	Technical Capabilities (C.2.5.1.1.4) [RIN: MTR0091-DN, MTR0123-DN]	106
2.1.2.5.1.1.4.1	Technical Capabilities of Private Cloud and community cloud (C.2.5.1.1.4.1).....	117
2.1.2.5.1.1.4.2	Technical Capabilities of Data Center Augmentation with Common Information Technology Service Management (itsm) (C.2.5.1.1.4.2)	117
2.1.2.5.1.2 ...	<i>Features (C.2.5.1.2)</i>	118
2.1.2.5.1.3 ...	<i>Interfaces (C.2.5.1.3)</i>	119
2.1.2.5.1.4 ...	<i>Performance Metrics (C.5.1.4)</i>	119
2.1.2.5.1.4.1	Cloud Data Center (C.5.1.4.1)	119
2.1.2.5.1.4.2	Transport to Cloud Data Center (C.5.1.4.2).....	121
2.1.2.5.2	PLATFORM AS A SERVICE (C.2.5.2)	122
2.1.2.5.3	SOFTWARE AS A SERVICE (C.2.5.3).....	122
2.1.2.5.4	CONTENT DELIVERY NETWORK SERVICES (C.2.5.4).....	122
2.1.2.6	Wireless Services (C.2.6)	122
2.1.2.7	Commercial Satellite Communications Services (C.2.7)	122
2.1.2.8	Managed Services (C.2.8)	123
2.1.2.8.1	MANAGED NETWORK SERVICE* (C.2.8.1)	123
2.1.2.8.2	WEB CONFERENCING SERVICE (C.2.8.2).....	123
2.1.2.8.3	UNIFIED COMMUNICATIONS SERVICE (C.2.8.3).....	123
2.1.2.8.4	MANAGED TRUSTED INTERNET PROTOCOL SERVICE (C.2.8.4)	123
2.1.2.8.5	MANAGED SECURITY SERVICES (C.2.8.5)	123
2.1.2.8.6	MANAGED MOBILITY SERVICE (C.2.8.6)	123
2.1.2.8.7	AUDIO CONFERENCING (C.2.8.7) [RIN: MTR0047-DN]	123
2.1.2.8.7.1 ...	<i>Service Description (C.2.8.7.1)</i>	123
2.1.2.8.7.1.1	Functional Definition (C.2.8.7.1.1).....	124
2.1.2.8.7.1.2	Standards (C.2.8.7.1.2) [RIN: MTR2242-DN].....	125
2.1.2.8.7.1.3	Connectivity (C.2.8.7.1.3)	125
2.1.2.8.7.1.4	Technical Capabilities (C.2.8.7.1.4) [RIN: MTC0017-DI, MTC0018-DI, MTC0019-DI, MTC0020-DI, MTC0021-DI].....	126

2.1.2.8.7.2... Features (C.2.8.7.2) [RIN: MTC0022-DI, MTC0023-DI, MTC0024-DI, MTC0025-DI, MTC0028-DI, MTR0072-DN, MTR2246-DN].....	130
2.1.2.8.7.3... Interfaces (C.2.8.7.3).....	132
2.1.2.8.7.4... Performance Metrics (C.2.8.7.4) [RIN: MTR0052-DN]	132
2.1.2.8.8 VIDEO TELECONFERENCING (C.2.8.8) [RIN: MTR0156-DN, MTR2243-DN].....	133
2.1.2.8.9 DHS INTRUSION PREVENTION SECURITY SERVICE (C.2.8.9)	133
2.1.2.9 Access Arrangements* (C.2.9)	133
2.1.2.10.... Service Related Equipment (C.2.10)	133
2.1.2.10.1 DEFINITION AND ONLINE CATALOG REQUIREMENT	134
2.1.2.10.2 WARRANTY SERVICE (C.2.10.1).....	134
2.1.2.10.3 RANGE OF SRE PRODUCTS PROVIDED	134
2.1.2.10.4 SOURCING PARTNERSHIP	136
2.1.2.11.... Service Related Labor (C.2.11) [RIN: MTR2217-DN].....	137
2.1.2.12.... Cable and Wiring (C.2.12) [RIN: MTR0159-DN]	137
2.1.2.12.1 SERVICE AND FUNCTIONAL DESCRIPTION	137
2.1.2.12.1.1. Standards	140
2.1.2.12.1.2. Connectivity	141
2.1.2.12.1.3. Interfaces	141
2.2 INFORMATION SECURITY (L.29.2.2)	141
2.3 EXTERNAL TRAFFIC ROUTING REQUIREMENT (L.29.2.3) [RIN: MTC0031-DI, MTC0004-DI, MTC0006-DI, MTC0007-DI, MTC0008-DI, MTC0009-DI, MTC0010-DI, MTR0109-DN, MTR0112-DN, MTR0121-DN, MTR0122-DN, MTR0111-KS]	141
2.3.1 Traffic identification and routing policy (C.1.8.8(3)).....	147
2.4 INTEROPERABILITY (C.1.8.6) [RIN: MTC0011-DI]	149
2.5 SYSTEM SECURITY (C.1.8.7) [RIN: MTR0132-DN, MTR0133-DN, MTR0135-DN, MTR0136-DN, MTR0137-DN, MTR0138-DN, MTR0139-DN]	149
2.5.1 System Security Compliance Requirements (C.1.8.7.1)	149
2.5.2 System Security Plan (SSP) (C.1.8.7.4)	160
2.5.3 Personnel Background Investigation Requirements (C.1.8.7.7) [RIN: MTC0032-DI].....	160

2.6	TECHNICAL SUPPORT (C.1.8.9) [RIN: MTC0030-DI].....	161
2.6.1	Customer Support Office and Technical Support (G.6.2)	161
2.6.2	Trouble Ticket Management (G.6.4).....	163
2.6.2.1 Trouble Ticket Management General Requirements (G.6.4.1)	163
2.6.2.2 Reporting Information (G.6.4.2)	163
2.7	MINIMUM REQUIREMENTS FOR GEOGRAPHIC COVERAGE (C.1.3).....	164
2.8	SECTION 508 REQUIREMENTS (C.4)	164
2.8.1	Voluntary Product Accessibility Template (C.4.2)	164
2.8.2	Section 508 Applicability to Technical Requirements (C.4.3).....	164
2.8.3	Section 508 Provisions Applicable to Reporting and Training (C.4.5)	164
3.0	RISK MANAGEMENT PLAN (G.9.4.10) [RIN: MTR0124-DN, MTR0147-DN, MTR0149-DN, MTR0150-DN, MTR0153-DN, MTR0154-DN]	165
3.1	CTI RISK MANAGEMENT PLAN FOR IDIQ AND TASK ORDERS	184
3.1.1	IDIQ Level Risk Management Plan and TO Risk Management Plan (NIST 800-37 R1)	184
3.1.1.1 Risk triggers	191
4.0	SUBMISSION MATRIX (L.29.2.4).....	0

Table of Figures

Figure 1: Core Technologies - "Core" Network Architecture	1
Figure 2: Long Haul Network	2
Figure 3: IP Assets	3
Figure 4: Local Voice.....	3
Figure 5: Service Providers	6
Figure 6: Redundant Paths Usage	15
Figure 7: VPNS network diagram.....	17
Figure 8: ETS network diagram.....	27
Figure 9: IPVS diagram (C.2.2.1)	44
Figure 10: MNS diagram	55
Figure 11: Access Arrangement diagram	70
<i>Figure 12: Access Arrangement Functional definition diagram</i>	<i>70</i>
Figure 13: QTS Data Center Services and Management Solutions.....	98
<i>Figure 14: Audio Conferencing Service Description</i>	<i>124</i>
Figure 15: Video Teleconferencing Service Definition.....	Error! Bookmark not defined.
Figure 16: Service Related Equipment	136
Figure 17: Cable and Wiring (2).....	139
Figure 18: Cable and Wiring (4).....	139
Figure 19: Cable and Wiring (3).....	140
Figure 20: Cable and Wiring (1).....	140
Figure 21: Sensing & Control Mechanisms.....	145
Figure 22: Risk Management Framework Process	167
<i>Figure 23: The SCRM Plan Tiers – CTI’s approach to Risk-Based decisions based on traceability, transparency, accountability and continuous improvement.</i>	<i>185</i>
<i>Figure 24: Enterprise/Project Setup – The CTI Team sets up every Contract and Task Order in the Risk Radar to monitor and assess the risks.</i>	<i>188</i>
<i>Figure 25: Opportunity Management – Every Task Order is assessed individually for its inherent risk factors.</i>	<i>189</i>

<i>Figure 26: Global Risk Characteristics – Allows to set up and monitor all risks by each characteristic.</i>	190
<i>Figure 27: Risk Project Milestone – Allows to stipulate and analyze the risk at each project milestone</i>	191
<i>Figure 28: Project Risk Triggers – Allows for triggers to be set up within the program to alert the appropriate personnel for an action or notification to take place.</i>	192
<i>Figure 29: Project User Permissions – Allows for the appropriate permissions settings at every level within the project.</i>	193
<i>Figure 30: Risk Details – Allows CTI to assign specific risk parameters for each risk.</i>	194
<i>Figure 31: Mitigation Steps – Allows to input risk mitigation characteristics for each risk type.</i>	194
<i>Figure 32: Association Screen – Allows for risk association within all projects/programs.</i>	195
<i>Figure 33: Project Risk Prioritization – Allows the risk prioritization as the environment or parameters change.</i>	196
<i>Figure 34: Risk State – Allows to view the exposure of each risk in case of a change in the environment or parameters.</i>	196
<i>Figure 35: Risk Reports – Standard Reports provide customers and internal personnel with a consolidated view of current risks.</i>	197
<i>Figure 36: Ad Hoc Reports - Allows customizable reports for specific issues and or risk factors.</i>	198

Table of Tables

<i>Table 1: VPNS Features table (C.2.1.1.2)</i>	25
<i>Table 2: VPNS Interfaces table (C.2.1.1.3)</i>	25
<i>Table 3: VPNS Performance Metrics table (C.2.1.1.4)</i>	26
<i>Table 4: ETS Interfaces table (C.2.1.2.3)</i>	39
<i>Table 5: ETS Performance Metrics table</i>	40
<i>Table 6: IPVS features table (C.2.2.1.2)</i>	50
<i>Table 7: IPVS Interfaces table</i>	51

Table 8: Performance Metrics (C.2.2.1.4)	52
Table 9: Services provided by Smart Reporting	66
Table 10: Access diversity and avoidance table (C.2.9.2)	78
Table 11: AA Interfaces diagram (C.2.9.3)	79
Table 12: Features (C.2.2.2.2)	88
Table 13: Interfaces (C.2.2.2.3)	89
Table 14: Performance Metrics (C.2.2.2.4)	89
Table 15: IaaS Reservation vs Stand-alone Model	94
Table 14: Cloud Data Center Performance Standards	120
Table 15: Cloud Data Service Length of Outage vs Service Level Credit	121
Table 18: Performance Metrics (C.2.8.7.4)	133
Table 16: Video Teleconferencing Interfaces table (C.2.8.8.3) Error! Bookmark not defined.	
Table 17: Video Teleconferencing Services Performance Metrics (C.2.8.8.4.1) Error! Bookmark not defined.	
Table 21: Smart Reporting Capabilities	144
Table 18: Risk Management Comprehensive Task List - The CTI Team's comprehensive list is applied to every contract and every Task Order.	186
Table 19: Risk Management Comprehensive Task List - The CTI Team's comprehensive list is applied to every contract and every Task Order.	187

Abbreviation or Acronym	Definition
A	
A&A	Assessment and Authorization
AA	Access Arrangement
ACO	Administrative Contracting Officer
ACS	Audio Conferencing Service
ACT	Accounting Control Transaction
AD	Agency Dispute
ADSL	Asymmetric DSL

AGF	Associated Government Fee
AGFD	AGF Detail
AHC	Agency Hierarchy Code
AHS	Application Hosting Services
AIS	Automated Information System
ANI	Automatic Number Identification
ANSI	American National Standards Institute
Anti-DDoS	Anti-Distributed Denial of Service
AO	Authorizing Official
AOW	Area of the World
API	Application Programming Interface
APS	Automatic Protection Switching
ARIN	American Registry for Internet Numbers
AQL	Acceptable Quality Level
AS	Autonomous System
ASC	Accredited Standards Committee
ASCII	American Standard Code for Information Interchange
ASCO	Adversarial Supply Chain Operation
ASON	Automatic Switched Optical Network
ASP	Applications Services Provider
ASRN	Agency Service Request Number
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
ATO	Authority to Operate
ATR	AGF Electronic Funds Transfer Report
AU	Authorized Users
AUP	Acceptable Use Policy
Av(S)	Availability (Service)
AVI	Audio Visual Interleave
AVM	Anti-Virus Management
AVMS	Anti-Virus Management Service
B	
B2B	Business to Business

BA	Billing Adjustment
BI	Billing Invoice
BER	Bit Error Rate
BGAN	Broadband Global Area Network
BGP	Boarder Gateway Protocol
BIA	Business Impact Assessment
BIT	Binary Digit
BLS	Bureau of Labor Statistics
BoD	Bandwidth on Demand
BLSR	Bidirectional Line Switched Ring
BPS	Bits per second
BPSR	Bidirectional Path Switched Ring
BRI	Basic Rate Interface
BSD	Boundary Scope Document
BSS	Broadband Switching System
BSS	Business Support System
BTN	Billing Telephone Number
BYOD	Bring Your Own Device
C	
CA	Criticality analysis
CAC	Common Access Card
CAGE	Commercial and Government Entity
CAP	Compliance and Assurance Program
CBAS	Central Billed Agency Setup
CBASR	Central Billed Agency Setup Reply
CBR	Constant Bit Rate
CBS	Committed Burst Size
CBSA	Core Based Statistical Area
CCCS	Customer Contact Center Services
CCE	Common Configuration Enumerations
CCS	Contact Center Service
CCV	Cybersecurity Compliance Validation
CDIP	Contractor Data Interaction Plan

CDMA	Code Division Multiple Access
CDN	Content Delivery Network
CDNS	Content Delivery Network Service
CDP	Carbon Disclosure Project
CDR	Call Detail Record
CDRL	Contract Deliverables Requirements List
CE	Customer Edge
CFR	Code of Federal Regulations
CFSS	Commercial Fixed Satellite Service
CGI-Bin	Common Graphic Interface - Binary
CID	Caller ID
CIR	Committed Information Rate
CIRs	Committed Information Rates
CIS	Center for Internet Security
CLIN	Contract Line Item Number
CLLI	Common Language Location Identifier
CLONES	Central Location Online Entry System (iconectiv database)
CMSS	Commercial Mobile Satellite Service
CNAM	Calling Name
CNM	Customer Network Management
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CO	Contracting Officer
COMSATCOM	Commercial Satellite Communication
CONUS	Continental United States
COOP	Continuity of Operations
COR	Contracting Officer's Representative
CoS	Class of Service
CoSS	Collaboration Support Services
COTS	Commercial off-the-shelf
CP	Contingency Plan
CPDF	Central Personnel Data File

CPE	Customer Premises Equipment
CPLG	Coupling
CPMO	Contractor's Program Management Office
CPTP	Contingency Plan Test Plan
CPTPR	Contingency Plan Test Plan Report
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSA	Communications Service Authorization
CSC	Customer Service Center
CSDS	Circuit Switched Data Service
CSO	Customer Support Office
CSP	Communications Service Provider
CSRN	Contractor Service Request Number
CSS	Circuit Switched Service
CSTA	Computer Supported Telephony Applications
CSU/DSU	Channel Service Unit/Data Service Unit
CSV	Comma-Separated Value
CSVS	Circuit Switched Voice Service
CTI	Computer Telephony Integration
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CW	Cable and Wiring
CWD	Customer Want Date
D	
D/A	Departments and Agencies
DBA	Doing Business As
DBAS	Direct Billed Agency Setup
DCC	Data Communications Channel
DCOM	Distributed Component Object Model
DCS	Data Center Service
DCSS	Digital Cross-Connect Systems
DDoS	Distributed Denial of Service
DES	Data Encryption Standard

DFS	Dark Fiber Service
DHCP	Dynamic Host Configuration Protocol
DHS	Dedicated Hosting Service
DID	Direct Inward Dial
DIS	Draft International Standard
DLCI	Data Link Connection Identifier
DLP	Data Loss Prevention
DLS	Data Link Switching
DM	Degraded Minutes
DMS	Defense Message System
DMZ	Demilitarized Zones
DNBH	During Normal Business Hours
DNI	Dialed Number Identification
DNIS	Dialed Number Identification Service
DNS	Domain Name System
DNSSEC	DNS Security Extensions
DoD	Department of Defense
DoDI	Department of Defense Instruction
DoS	Denial of Service
DPA	Delegation of Procurement Authority
DR	Disaster Recovery
DR	Dispute Report
DSL	Digital Subscriber Line
DSN	Defense Switched Network
DSSR	Department of State Standardized Regulations
DSU	Data Service Unit
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-Frequency
DUNS	Data Universal Numbering System
DWDM	Dense Wavelength Division Multiplexing
E	
EAD	Enterprise Active Directory
ECS	Electronic Commerce Service

EFMA	Ethernet in the First Mile Alliance
EFS	Error Free Seconds
EFT	Electronic Funds Transfer
E-Gov	Electronic Government
EIA	Electronic Industries Association
EIA/TIA	Electronic Industry Alliance/Telecommunications Industry Association
EIS	Enterprise Infrastructure Solutions
EIT	Electronic and Information Technology
E-LAN	Ethernet Private Local Area Network
E-LINE	Ethernet Private Line
EM	Element Manager
EMI	Electro-Magnetic Interference
EMS	Element Management Systems
EN	Event Notification
EO	Executive Order
EP	Emergency Preparedness
EPA	Environmental Protection Agency
ERM	E-mail Response Management
ERP	Enterprise Resource Planning
ESCON	Enterprise System Connection
ESF	Extended Superframe
ESI	Electronically Stored Information
ETL	Extract, Transform and Load
ETS	Ethernet Transport Service
ETSI	European Telecommunications Standards Institute
EVC	Ethernet Virtual Connection
F	
FAR	Federal Acquisition Regulation
FB	Fixed Bandwidth
FCC	Federal Communications Commission
FCCI	Federal Cloud Computing Initiative
FCIA	Fiber Channel Industry Association
FDCCI	Federal Data Center Consolidation Initiative

FDP	Fiber Distribution Panel
FEDBIZOPPS	Federal Business Opportunities
FedRAMP	Federal Risk and Authorization Management Program
FED-STD	Federal Standard
FedVRS	Federal Video Relay Service
FEMP	Federal Energy Management Program
FICON	Fiber Connectivity
FIPS	Federal Information Processing Standard
FIPS 200	Federal Information Processing Standards Publication 200
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
FLSA	Fair Labor Standards Act
FOC	Firm Order Commitment
FOCN	Firm Order Commitment Notice
FOIA	Freedom of Information Act
FS	Federation Services
FSDP	Fiber Service Delivery Point
FT1	Fractional T1
FT3	Fractional T3
FTP	File Transfer Protocol
FTR	Federal Telecommunications Recommendations
FOTP	Fiber to the Premises
FUSF	Federal Universal Service Fund
G	
GAO	General Accounting Office
GB	Gigabyte
Gbps	Gigabit per second
GETS	Government Emergency Telecommunications Service
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFP	Government Furnished Property
GFP	Generic Framing Procedure
GMPLS	Generalized Multi-Protocol Label Switching

GOS	Grade of Service
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GRI	Global Reporting Initiative
GSA	General Services Administration
GSAR	GSA Regulation
GUI	Graphical User Interface
H	
HCM	Human Capital Management
HF	High Frequency
HIDS	Host-based IDS
HR	Human Resources
HSPD-12	Homeland Security Presidential Directive-12
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol
HVAC	Heating, Ventilation and Air Conditioning
I	
IA	Interagency Agreement
IaaS	Infrastructure as a Service
ICB	Individual Case Basis
ICE	Interactive Connectivity Establishment
ICMP	Internet Control Message Protocol
ID	Identification (User)
IDC	Internet Data Center
IDE	Integrated Development Environment
IDPS	Intrusion Detection and Prevention Service
IDS	Intrusion Detection System
IDSL	ISDN DSL
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IETF RFC	IETF Request for Comment

IMAP	Internet Message Access Protocol
INRS	Incident Response Service
IP	Internet Protocol
IPFIX	IP Flow Information Export
IPMS	Integrated Performance Monitoring Service
IPS	Internet Protocol Service
IPSec	IP Security
IPS	Intrusion Prevention Systems
IPSS	Intrusion Prevention Security Service
IPVS	Internet Protocol Voice Service
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IR1-SLM	Intermediate Reach Single Longitudinal Mode
IR	Inventory Reconciliation
IRP	Incident Response Plan
IRS	Internal Revenue Service
IRU	Indefeasible Rights of Use
ISA	Interconnection Security Agreements
ISCM	Information Security Continuous Monitoring
ISDN	Integrated Services Digital Network
ISDN BRI	ISDN Basic Rate Interface
ISM	In-Service Monitoring
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSM	Information Systems Security Manager
ISSO	Information System Security Officer
ISV	Independent Software Vendor
ITIL	IT Infrastructure Library
ITS	Integrated Technology Services
ITSM	IT Service Management
ITT	Information Technology Tools
ITU	International Telecommunications Union

ITU-TSS	International Telecommunications Union-Telecommunications Service Sector
IVR	Interactive Voice Response
K	
KPI	Key Performance Indicator
L	
L2TP	Layer 2 Tunneling Protocol
L3VPN	Layer 3 Virtual Private Network
LAN	Local Area Network
Latency(S)	Latency (Service)
LCAS	Link Capacity Adjustment Scheme
LDAP	Lightweight Directory Access Protocol
LEC	Local Exchange Carrier
LGC	Local Government Contact
LH	Long Haul
LLDS	Link Layer Data Service
LNP	Local Number Portability
LOA	Letter of Authorization
LOH	Line Overhead
LR1-SLM	Long Reach Single Longitudinal Mode
LSA	Local Service Agreement
LSP	Label Switched Paths
LTE	Long Term Evolution
M	
M2M	Machine to Machine
MACD	Moves, Adds, Changes, Disconnects
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MAS	Mobile Application Store
MB	Megabyte
MBI	Minimum Background Investigation
Mbps	Megabit per second
MBS	Maximum Burst Size

MCM	Mobil Content Management
MDM	Mobile Device management
MEF	Metro Ethernet Forum
MFS	Managed Firewall Service
MIL-STD	Military Standard
MIME	Multipurpose Internet Mail Extensions
MLPP	Multi-Level Precedence and Preemption
MMC	Monthly Maintenance Charge
MMF	Multi-Mode optical Fiber
MMRC	Maintenance Monthly Recurring Cost
MMS	Multimedia Messaging Service
MNS	Managed Network Service
MOS	Mean Opinion Score
MPIN	Marketing Partner Identification Number
MPLS	Multi-Protocol Label Switching
MPS	Managed Prevention Service
MRC	Monthly Recurring Charges
MRG	Minimum Revenue Guarantee
MS	Microsoft
MSS	Managed Security Service
MTIPS	Managed Trusted Internet Protocol Service
MTTLBCI	Mean Time to Loss of BCI
MUX	Multiplexer
MWS	Wireless Service
N	
NACI	National Agency Check with Written Inquiries
NACSZ	Name, Address, City, State, Zip code
NAICS	North American Industry Classification System
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NCPS	National Cyber Protection System Sensor
NCS	National Communications System

NDA	Non-Disclosure Agreement
NEBS	Network Equipment-Building System
NFC	Near Field Communication
NFS	Network File Systems
NFV/SDN	Network Function Virtualization and Software Defined Network
NIC	Network Interface Card
NIDS	Network Intrusion Detection Devices
NIS	Network Information Service
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NLT	Not Later Than
NMS	Network Management System
NNI	Network to Network Interface
NOC	Network Operations Center
NPA	Numbering Plan Area
NPA/NXX	Numbering Plan Area / Numbering Plan Exchange
NRC	Non-Recurring Charge
NS	National Security
NS/EP	National Security and Emergency Preparedness
NS2020	Network Services 2020
NSA	National Security Agency
NSC	Network Site Code
NSP	Not Separately Priced
NTSC	National Television Standards Committee
NUI	Network User Identification
NVF	Network Function Virtualization
NXX	Numbering Plan Exchange
NZDS	Non-Zero Dispersion Shifted
O	
O&S	Operations and Support
O*NET	Occupational Information Network
OADM	Optical Add-Drop Multiplexer
OAM	Operations, Administration and Management

OAM&P	Operations, Administration, Maintenance and Provisioning
OCN	Operating Company Number
OCO	Ordering Contracting Officer
OCONUS	Outside Contiguous United States
OCWR	Optical Continuous Wave Reflectometry
OEC	Office of Emergency Communication
OEM	Original Equipment Manufacture
OFCS	Optical Fiber Communications System
OFSTP	Optical Fiber System Test Procedure
OIF	Optical Internetworking Forum
OLP	Official List Price
OMB	Office of Management and Budget
ONBH	Outside Normal Business Hours
OOS	Out-Of-Service
OPM	Office of Personnel Management
OS	Operating System
OSAISO	Office of the Senior Agency Information Security Officer
OTDR	Optical Time-Domain Reflectometer
OTM	Optical Terminal Multiplexer
OTN	Optical Transport Network
OVF	Open Virtualization Format
OVPN	Optical Virtual Private Network
OWS	Optical Wavelength Service
P	
P&P	Policies and Procedures
PaaS	Platform as a Service
PAL	Phase Alternation by Line
PAT	Port Address Translation
PBX	Private Branch Exchange
PC	Personal Computer
PCL	Physical Concentration Location
PDF	Portable Document Format
PDU	Protocol Data Unit

PHub	Pricing Hub
PIA	Privacy Impact Assessment
PIC	Presubscribed Interexchange Carrier
PIDF	Presence Information Data Format
PII	Personally Identifiable Information
PIID	Procurement Instrument Identifier
PIM	Personal Information Management
PIN	Personal Identification Number
PIR	Peak Information Rate
PIV	Personal Identity Verification
PKI	Public Key Encryption
PLS	Private Line Service
PM	Performance Monitoring
PMD	Polarization Mode Dispersion
PMO	Program Management Office
PMP	Program Management Plan
POA&M	Plan of Action and Milestones
POC	Point of Contact
PoE	Power over Ethernet
PON	Passive Optical Networks
POP	Point of Presence
PPIRS	Past Performance Information Retrieval System
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
PSTN	Public Switched Telephone Network
PTT	Push to Talk
PVC	Permanent Virtual Circuit
PWE	Pseudo Wire Emulation
PWE3	Pseudo Wire Emulation Edge to Edge
PWS	Performance Work Statement

Q	
QA	Quality Assurance
QoS	Quality of Service
QPMR	Quarterly Program Management Review
R	
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
RFC	Request for Comment
RFI	Request for Information
RFI	Radio Frequency Interference
RFP	Request for Proposal
RFQ	Request for Quotation
RMF	Risk Management Framework
RoB	Rules of Behavior
RPC	Remote Procedure Call
RPR	Resilient Packet Rings
RT	Response Time
RTP	Real-Time Transport Protocol
RTT	Radio Transmission Technology
S	
SaaS	Software as a Service
SAM	System for Award Management
SAN	Storage Area Networks
SAR	Security/Risk Assessment Report
SC(O)	Switched Connection (Optical)
SCAP	Security Content Automation Protocol
SCCP	Skinny Client Control Protocol
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCOM	System Center Operations Manager
SCRM	Supply Chain Risk Management
SD	Signal Degradation
SDH	Synchronous Digital Hierarchy

SDK	Software Development Kit
SDN	Software Defined Network
SDP	Service Delivery Point
SDS	Switched Data Service
SDSL	Symmetric DSL
SECAM	Système Electronique Couleur Avec Memoire
SES	Severely Errored Seconds
SF	Super Frame
SF	Signal Failure
SFTP	Secure File Transport Protocol
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SIS	Satellite Internet Service
SLA	Service Level Agreement
SLACR	SLA Credit Request
SLACRR	SLA Credit Request Response
SLAR	SLA Report
SMB	Server Message Block
SME	Subject Matter Expert
SMF	Single Mode optical Fiber
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SO	Service Order
SOA	Service Order Acknowledgement
SOAC	Service Order Administrative Change
SOC	Security Operations Center; Service Order Confirmation
SOCN	Service Order Completion Notice
SORN	Service Order Rejection Notice
SOH	Section Overhead
SONET	Synchronous Optical Network
SONET ADM	SONET Add-Drop Multiplexer
SOO	Statement of Objective
SOW	Statement of Work

SP	Special Publication
SR	Short Reach
SRE	Service Related Equipment
SRG	Security Requirements Guide
SR-MLM	Short Reach Multi-Longitudinal Mode
SS	Storage Service
SSCN	Service State Change Notice
SSH	Secure Shell
SSL	Secure Sockets Layer
SSL/TLS	Secure Sockets Layer/Transport Layer Security
SSM	Synchronous Status Messaging
SSP	System Security Plan
STP	Shielded Twisted Pair
STUN	Session Traversal Utilities for NAT
SVC	Switched Virtual Circuit
SWC	Serving Wire Center
SWOT	Strengths, Weaknesses, Opportunities and Threats
T	
TACACS	Terminal Access Controller Access Control System
TAX	Tax Detail
TB	Terabyte
TBD	To Be Determined
TCP/IP	Transmission Control Protocol/Internet Protocol
TDD	Telecommunications Device for the Deaf
TDD/TTY	Telecommunications Device for the Deaf/Teletypewriter
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TEMS	Telecommunications Expense Management Service
TESP	Telecommunications Electric Service Priority
TFS	Toll Free Service
TICAP	Trusted Internet Connection Access Provider
TIC	Trusted Internet Connection
TIN	Taxpayer Identification Number

TLS	Transport Layer Security
TMSAD	Trust Model for Security Automation Data
TO	Task Order
TOH	Transport Overhead
TOPP	Task Order Project Plan
TP	Transition Plan
TSGR	Transport Systems Generic Requirements
TSMP	Transition Strategy and Management Plan
TSP	Telecommunications Service Priority
TS/SCI	Top Secret/Sensitive Compartmented Informaiton
TTR	Time to Restore
TUC	Task Order Unique CLIN
U	
UBI	Unique Billing Identifier
UCS	Unified Communications Service
UI	User Interface
UIFN	Universal International Free Phone Number
UM	Unified Messaging
UMTS	Universal Mobile Telecommunications System
UNI	User-to-Network Interface
UPS	Uninterruptible Power System
UPSR	Unidirectional Path Switched Ring
URL	Universal Resource Locator
USC	United States Code
US-CERT	United States Computer Emergency Readiness Team
USDA	United States Department of Agriculture
UTC	Coordinated Universal Time
UTP	Unshielded Twisted Pair
V	
V&H	Vertical and Horizontal
VBR	Variable Bit Rate
VESDA	Very Early Smoke Detection Apparatus
VM	Virtual Machine

VoIP	Voice over Internet Protocol
VoIPTS	Voice over Internet Protocol Transport Service
VPAT	Voluntary Product Accessibility Template
VPN	Virtual Private Network
VPNS	Virtual Private Network Service
VS	Voice Service
VSAT	Very Small Aperture Terminal
VSR	Very Short Reach
VSS	Vulnerability Scanning Service
VT	Virtual Tributary
VTN	Virtual Telephone Number
VTS	Video Teleconferencing Service
VXML	Voice Extensible Markup Language
W	
WAN	Wide Area Network
WAP	Wireless Application Protocol
WCS	Web Conferencing Service
WDM	Wavelength Division Multiplexing
WEP	Wired Equivalent Privacy
WFM	Workforce Management
WLAN	Wireless Local Area Network
WMI	Windows Management Instrumentation
WPA	Wi-Fi Protected Access
WPS	Wireless Priority Service
WSDL	Web Service Definition Language
WWW	World Wide Web
X	
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
XSD	XML Schema Definition
XTACACS	Extended TACACS

1.0 NETWORK ARCHITECTURE (L.29.1) [RIN: MTR0102-DN]

1.1 UNDERSTANDING

Core Technologies (“CTI”) is a Telecommunication Wholesale Aggregator that provides a comprehensive, end-to-end telecommunications solution. From carriers, cloud and IP infrastructure services, to legacy & advanced services, to issue resolutions and every matter in between -- we do it all. CTI provides a dedicated team of customer service and technical specialists who can easily service and manage various customers, regardless of customer’s locations, in a single report and in one Consolidated Invoice.

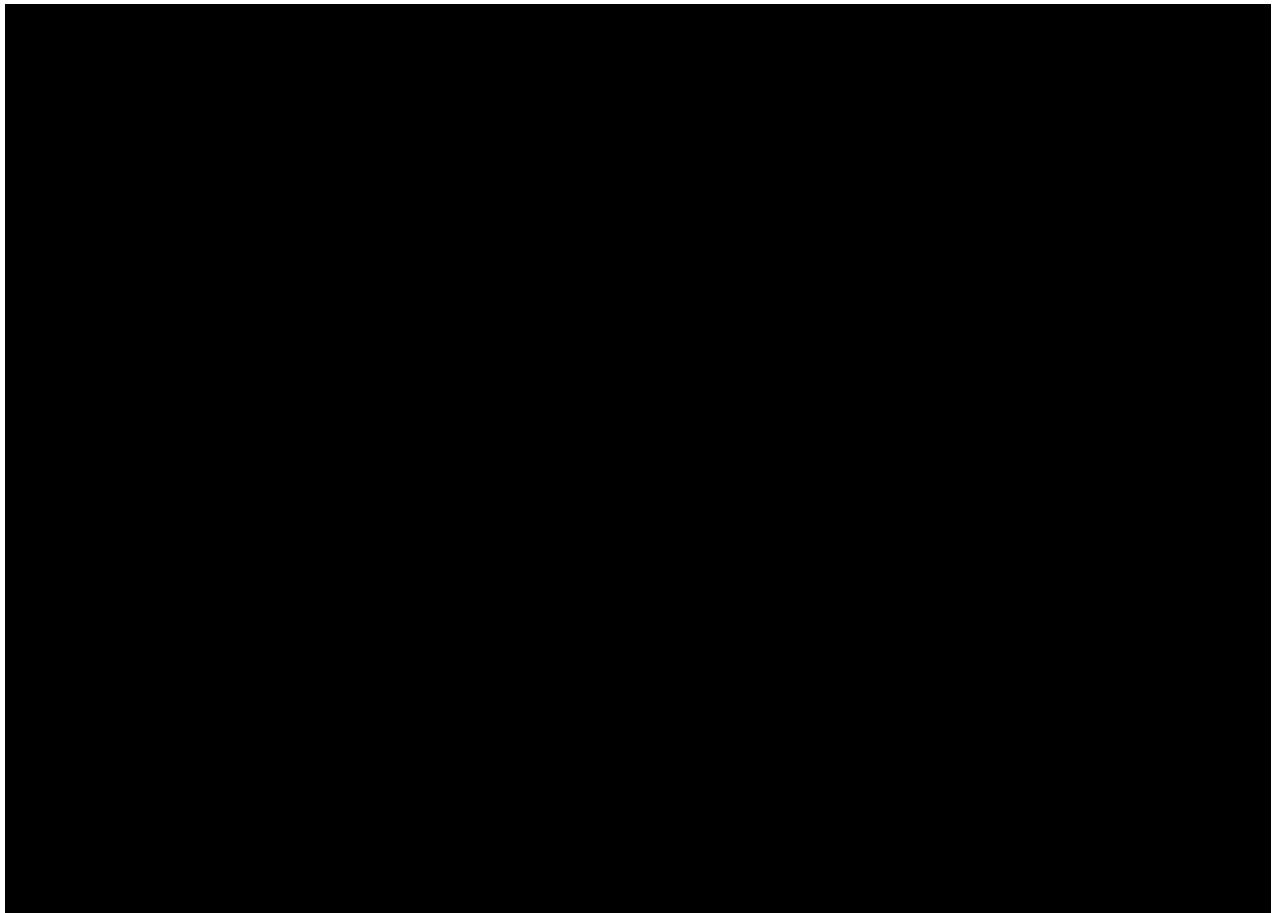
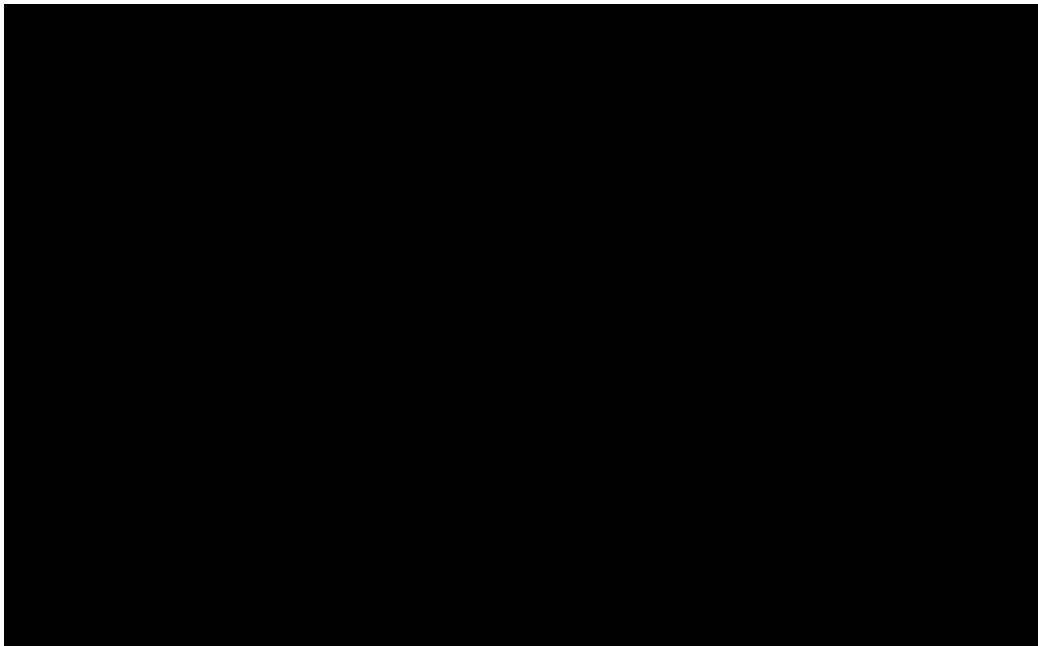


Figure 1: Core Technologies - "Core" Network Architecture

The network architecture diagram (Figure 1) illustrates a mesh of multiple 10 Gigabit (Gbps) circuits, connecting network nodes, peering POPs and Data Centers nationwide. The IP backbone runs across its own intercity fiber facilities, supported by terabit-capable core routing platforms and high-capacity peering interconnections.

CTI offerings provide Dedicated Internet Access (DIA) and IP Transit customers enhanced Internet connectivity. This network design delivers maximum end-to-end throughput as well as high levels of protection, redundancy, and Quality of Service required to support Voice over IP services. The IP network utilizes an advanced IP design, ensuring scalability as well as the ability to offer advanced future IP services plus the added benefit of no single IP point of failure past the customer access port.

Service delivery provided for “the last hundred miles” for each of the 931 CBSA’s is via CTI’s through sourcing logistics including local providers, and in the case of OCONUS or remote areas through SATCOM services should that option be proposed and activated.



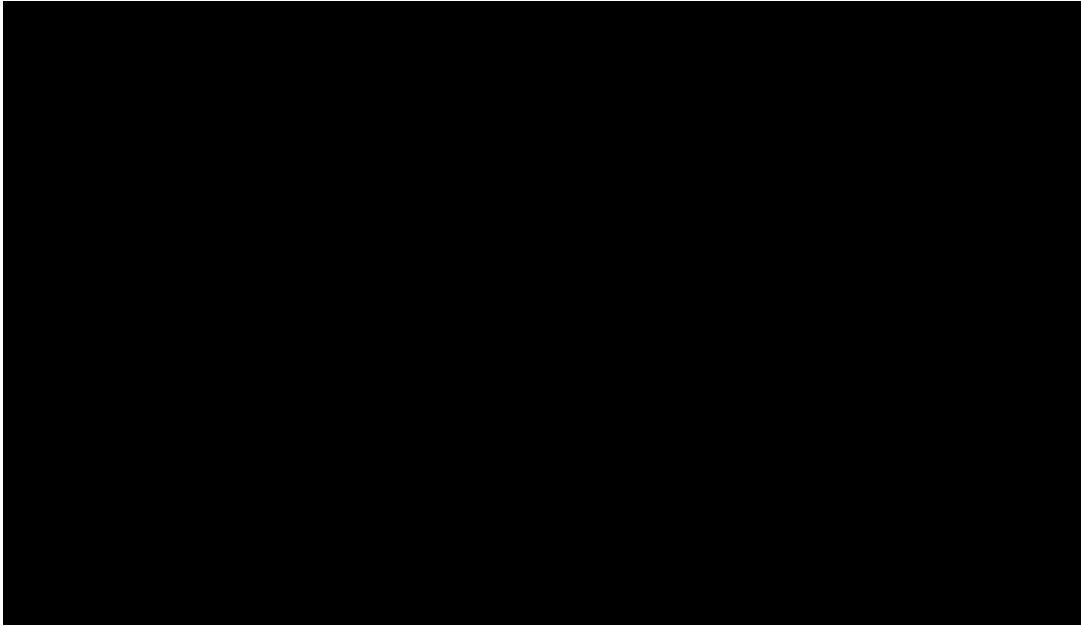


Figure 3: IP Assets

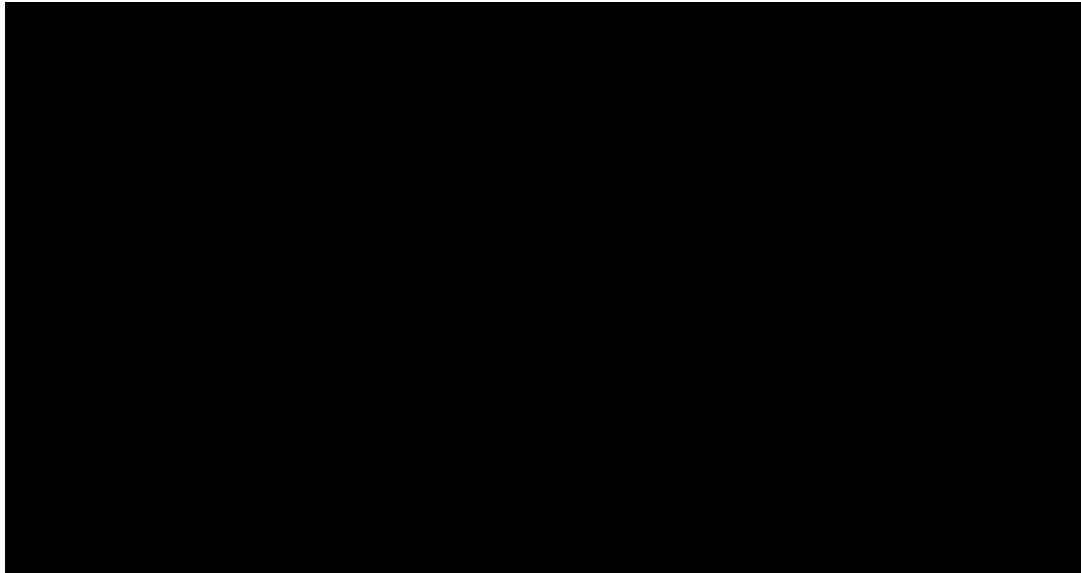


Figure 4: Local Voice

[REDACTED]

As a wholesale aggregator, CTI is a single source for all your telecommunications needs. We do all of the leg work with the existing agreements/business relationships, and requirements, while being prices competitive as a wholesale aggregator. [REDACTED]

[REDACTED]

Wholesale Aggregation Services:

CTI Wholesale Aggregation Service provides connectivity access to the PSTN and Internet cloud for small agency locations or agency locations that are not located in major concentration areas of the country.

Wholesale Aggregation provides the following services:

1. Service Availability (Pre-Qualifications)

Service Availability- is performed in accordance with the customer's preferences as specified in the service request and/or marketing survey.

2. Order Management-Installation

Service Order Placement- Orders will be placed with the appropriate service provider. The customer must execute an appropriate Letter of Agency. Installation times and dates must be agreed to by both parties.

3. Test and Turn-Up

Coordination with the service-provider and customer designated point of

contact are scheduled. Site surveys have been completed and an agreed time of test and turn-up is executed and preformed.

4. **End User Support** – 24 hour monitoring and alert notifications

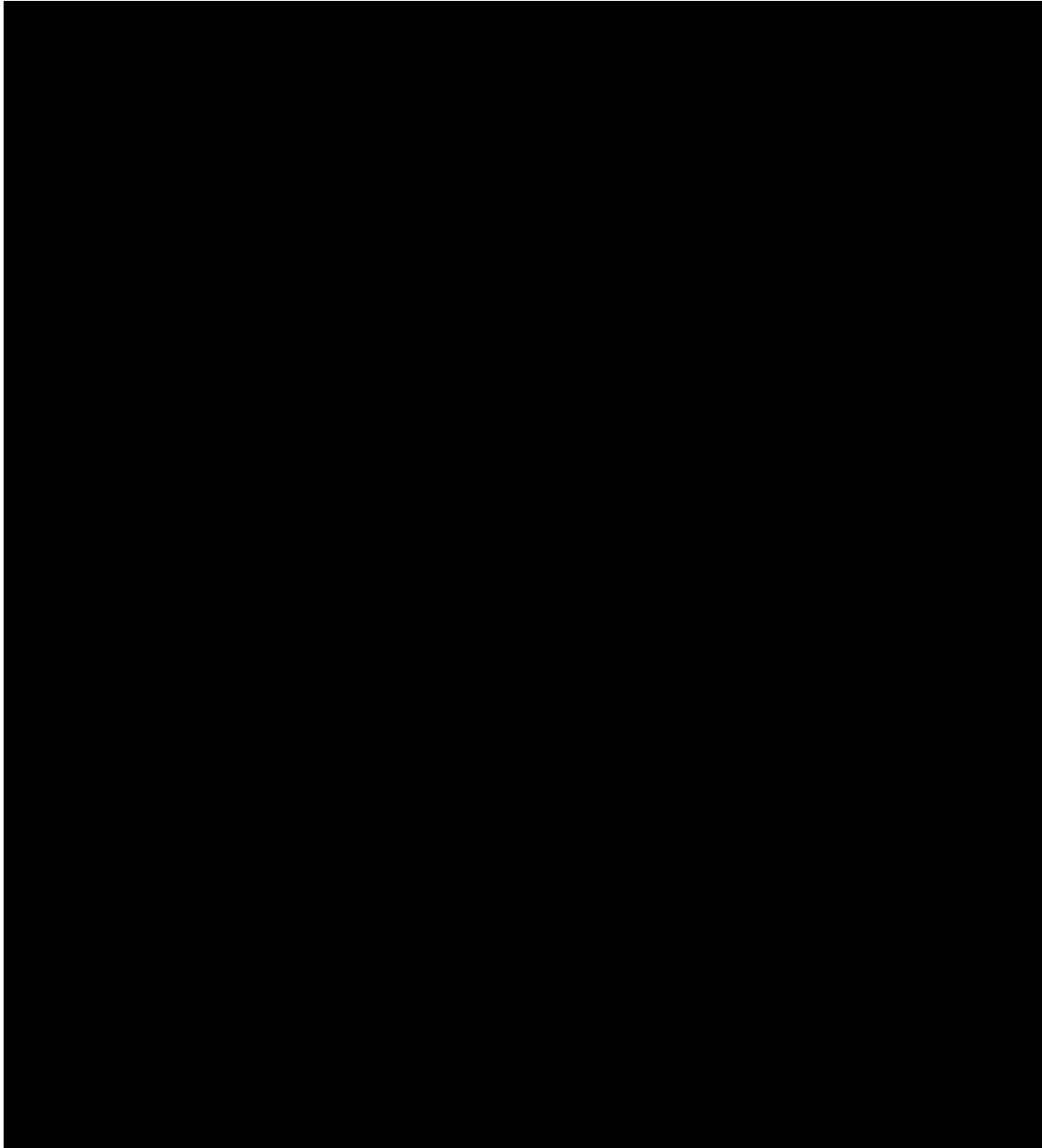
All circuits and services are monitored and any alerts can be routed to appropriate persons emails for notifications.

5. **Hardware Provisioning**

6. **Hardware Support Services Broadband Service Provisioning**

Tech Support is provided related to communication services. This includes private and Internet connectivity, virtual private network (VPN), voice over Internet protocol (VoIP), wireless fidelity (Wi-Fi). All Tech Support is telephone-based and is provided on a 5x8 basis.

Service Providers currently available hereunder include but is not limited to:



1.2 QUALITY OF SERVICES

CTI network architecture is designed for the complex and security sensitive needs of agencies and meets deliverability, compliance, scalability, reliability, and resilience standards outlined in each EIS service.

CTI's service networks are developed and offers strong QoS guarantees. The selective use of networks which are providing services of the highest QoS can be increased by several factors, one of which is being able to select the best provider, while keeping this activity transparent to the customer. The customer requires the bandwidth at a given price and CTI ensures that the customer receives what they pay for without requiring the customer to decide the details. The CTI interconnection structure also strongly influences the efficiency and QoS of an ISP and CTI ensures that the ISP selected has strong network interconnection structures that are connected with our peering and transit networks. CTI also uses traffic engineering to further improve the efficiency and QoS obtained with the network architecture and CTI also analyses the interconnections. Weaknesses in existing approaches are identified and corrected. Capacity expansion is deemed to be one of the more important network engineering tasks that CTI will have and CTI conducts traffic engineering analysis along with its vendors and ISP providers when planning capacity expansions.

1.3 SERVICE COVERAGE [RIN: MTR2249-KS]

CTI consolidated Network Architecture combined with our wholesale aggregation services will provide a comprehensive suite of telecommunications service covering 909 of the CBSA areas. The combined following access:

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

1.4 SECURITY [RIN: MTR0114-DN]

CTI's architecture and services comply with security specifications as identified in the following:

- a) CTI meets service-specific requirements as defined at both the proposal and TO level. CTI also possesses the resources to adapt security needs on a post-award as-needed basis.
- b) CTI provides security designed for traffic of varying levels of sensitivity, including Top Secret/SCI and encrypted data by agency users. CTI network services, information, infrastructure, and information processing resources are all shielded from security threats and system failures.
- c) CTI meets the external traffic routing requirements described in Section C.1.8.8, sub-paragraph 3, which include:
 - 1. The methodology for identifying the offeror's participating agency traffic for each affected service.
 - 2. Anticipated technical approach, for each affected service, to redirect all participating agency Internet, Extranet, and inter-agency traffic to DHS EINSTEIN Enclaves, receive processed traffic from GFP within the DHS EINSTEIN Enclave, and deliver traffic to its final destination.
 - 3. The technical approach to notify DHS should any non-participating agency traffic (IPv4, IPv6, etc.) be redirected through DHS EINSTEIN Enclaves.
 - 4. Control mechanisms the offeror will use to ensure that the identification and redirection of participating agency traffic is not inadvertently or maliciously bypassable.

5. Sensing and control mechanisms the offeror will use to ensure the redirection of traffic is failsafe (no disruption of participating agency services) should failures occur with DHS GFP.
6. The location of the offeror's existing or planned ANSI/TIA-942 and ICD 705 certified facilities that can serve as DHS EINSTEIN Enclaves capable of hosting DHS GFP at or near appropriate traffic-access locations.
7. Availability of TS/SCI-cleared personnel for "smart-hands" service of DHS supplied equipment.
8. Instrumentation to measure transport SLA KPIs (as if traffic passes through loopbacks in EINSTEIN Enclaves with no impact within DHS GFP being counted against the offeror's performance).

CTI will identify necessary hardware and firmware needed to provide and support the enterprise traffic/services in accordance with EIS GSA Solicitation Section C.1.8.8 sub-para (3) so that transportation (participating traffic) between the agency traffic collection point(s) -- physical or virtual -- and the EINSTEIN enclave can occur. Participating traffic is defined as the external traffic identified as part of the Traffic Aggregation Service (i.e. DHS Task Order); and routed to and delivered from a DHS EINSTEIN enclave (i.e. DHS chosen secure locations). Participating agency traffic network traffic is defined by the list of IP addresses and non-IP sources supplied by each agency and verified by DHS. Non-IP sources are converted to IP to be routed.

CTI will ensure that there is no way for participating traffic to inadvertently or maliciously bypass DHS EINSTEIN enclaves, by integration testing in a test environment before merging change into the production environment. The exception will be for failsafe service during times the DHS EINSTEIN enclave is not working, which should be minimized as CTI shall provide redundant paths for Agency traffic to EINSTEIN enclaves to ensure no loss of traffic occurs due to a component failure. This will necessitate more than one ENSTEIN enclaves at CTI facilities. Traffic Filtering and Traffic Prioritization shall occur in the routers of the CTI supported and maintained

network. EINSTEIN enclaves shall be hosted within CTI SCIFs or controlled, limited access network cages which are environmentally controlled/protected at CTI Headquarters or within approved team partner sites.

All traffic is aggregated and routed using Access Control Lists and VLAN tags. Traffic received from Participating Agencies will be identified, tagged with VLANs and forwarded to EINSTEIN enclaves. Traffic received from Non-participating will be forwarded to their final destinations. Traffic received from EINSTEIN enclaves, including traffic designated by the EINSTEIN enclave for delivery to US CERT, will be forwarded to their final destinations.

QoS features and rules can be assigned to traffic to prioritize routing. However, if the government furnished equipment in a DHS EINSTEIN enclave fails for whatever reason; CTI shall ensure redirection of traffic is failsafe, and return the participating traffic to its normal traffic path until the DHS EINSTEIN enclave is repaired.

CTI provided and supported hardware and firmware components include but are not limited to routers and switches, encryption devices, CSUs/DSUs, hubs, adapters, and modems, and the controlled EINSTEIN enclaves (s) which are used to receive traffic coming from DHS approved ISPs.

CTI will identify network components and determine protocols, redundancy, traffic filtering and traffic prioritization requirements, recommending the appropriate performance levels and network capacities as required and also meet applicable routing requirements in the GSA EIS solicitation Section C.1.8.8., such as:

1. CTI will provide multiple tunneling standards, as required by an agency. Examples include L2TP, GRE, IP-in-IP, MPLS, IPSec, and SSL/TLS.

-
2. CTI will provide various encryption levels, as required by an agency.
Examples include 3DES, RC4 and AES in accordance with the appropriate FIPS publications and modules.
 3. CTI will provide authentication services as required by an agency. Examples include RADIUS, Internal LDAP, token integration, PKI, and X.509 certificates.
 4. CTI will support IPv4 as both the encapsulating and encapsulated protocol.
 5. CTI will support IPv6 as both the encapsulating and encapsulated protocol.
 6. CTI will support QoS in the following standardized modes:
 - a. Best effort
 - b. Aggregate Customer Edge (CE) Interface level QoS (“hose” level)
 - c. Site-to-site level QoS (“pipe” level)
 - d. Intserv (RSVP) signaled
 - e. Diffserv marked
 7. CTI will support QoS across a subset of the access networks as listed below:
 - a. 802.1p Prioritized Ethernet
 - b. MPLS-based access
 - c. Multilink Multiclass PPP
 - d. QoS-enabled wireless:
 - i. LTE
 - ii. Wireless 802.11.x
 - iii. Cable high-speed access (DOCSIS 1.1)
 - iv. QoS-enabled Digital Subscriber Line (DSL)
 - v. QoS-enabled Satellite Broadband Access
 8. CTI will support one or more of the following application level QoS objectives:
 - a. Intserv model for selected individual flows
 - b. Diffserv model for aggregated flows
 9. CTI will provide isolation of traffic and routing service that isolates the exchange of traffic and routing information to only those sites that are authenticated and authorized members of a VPN. CTI will provide Multi-
-

Layered security architecture to ensure that attackers will not find a single point of entry but will be faced with multiple levels of security.

10. CTI will support multiple VPNs by allowing both permanent and temporary access to one or more VPNs for authenticated users across a broad range of access technologies using a variety of COTS products that meet the specific need of government customers.
11. CTI will provide secure routing services to provide full routing capability on the VPN platform with a secure policy across the VPN.
12. CTI will support the inclusion of encryption, decryption, and key management profiles as part of the security management system. Please see the section titled, "Managed Security Services" section 2.1.3.8.7 of this document.
13. CTI will support an agency in deploying its own internal security mechanisms in addition to those deployed by CTI, in order to secure specific applications or traffic at a granularity finer than a site-to-site basis.

CTI will assume responsibility for maintaining and repairing the traffic aggregation service, including associated commercial security services and all communications links, and shall provide engineering support [REDACTED]

[REDACTED]

Additionally, CTI shall, in accordance with EIS GSA Solicitation Section C.1.8.8 sub-para (3), ensure that services delivered are in compliance with national policy directives

that apply to the national telecommunications infrastructure such as national policy requirements that include, but are not limited to:

1. 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. CTI shall comply with NS/EP requirements as covered in Section G.11 of the GSA EIS Solicitation.
2. OMB Memorandum M-05-22 and OMB Memorandum M-09-32, "Update on the Trusted Internet Connections Initiative," "requires all agencies to undertake immediate responsibility for executing essential agreements and updating POA&Ms to facilitate not only TIC preparations, but also due diligence for integrating the National Cyber Protection System (NCPS, operationally referred to as EINSTEIN) deployments and synchronizing with US-CERT," and OMB Memorandum M-15-01, "Fiscal year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices" requires Departments and Agencies (D/As) to enter into legally sufficient agreements with DHS relating to the deployment of EINSTEIN. DHS establishes these agreements with D/As authorizing in-line traffic inspection and modification, and such activities may include the interception, modification, use, and disclosure of D/A traffic. As such, specific EIS data service offerings: VPNS, Ethernet Transport, PLS, IPS, Cloud services, which includes IaaS Private Cloud, PaaS, and SaaS, MNS Traffic Aggregation Service, MTIPS, and IPSS, and in future implementations could include other externally routed data services (e.g. OWS, SONETS), transporting Internet, Extranet, and Inter-Agency traffic shall identify and route said government traffic through a secure DHS EINSTEIN Enclave for processing by the latest generation of EINSTEIN capabilities. CTI shall design, implement, and operate its services to achieve the required routing of traffic through (including delivery to and receipt of traffic from) DHS EINSTEIN Enclaves. Transport SLA KPIs are measured as if through loopbacks in EINSTEIN Enclaves. EINSTEIN Enclaves are strictly intermediate hops and shall not be considered end points for SLA measurement. These contractor-performed actions related to EINSTEIN--

whether performed for DHS, GSA, or customer agencies--are intended to be assistance provided to the Secretary of DHS in accordance with 6 U.S.C. § 151.

To deliver appropriate hardware and firmware (e.g., routers, switches, and other SRE), related software, and SRL required to deliver the EIS services, CTI uses its partners and requesting agency infrastructure, as well as, commercially and government provided equipment such as EINSTEIN enclaves, to deliver the appropriate level of performance throughout the network services. [REDACTED]

[REDACTED] CTI shall identify necessary hardware and firmware needed to support the enterprise traffic in accordance with EIS GSA Solicitation Section C.1.8.8 sub-para (3) coming from the ISPs that has been identified per the approval of DHS as Agency traffic. The traffic furnished by the ISPs will be scanned for malware, viruses and all other malicious data such as bogus email accounts used in hacking prior to entering the EIS. The unwrapping of IP packets is done by the ISP and the DHS EINSTEIN enclave but Deep Packet Inspection occurs on in the DHS EINSTEIN enclave. If the IP packets prove to be without malicious content, then the DHS EINSTEIN enclave will reroute the data back to CTI which will send it back to the ISPs to be distributed to the proper agency(ies). If non-participating traffic gets routed to DHS EINSTEIN enclave the ISPs will notify the US-CERT of the infraction. The ISPs have the IP ranges of each Agency and it is their responsibility to alert US-CERT if an out of range IP address is routed to the DHS GFP.

[REDACTED] These types of connections vary depending on how the Circuit provider transports the traffic to the Network. The use of fiber using Dense Wavelength Division Multiplexing (DWDM), Multiprotocol Label Switching (MPLS), Copper Wire (ISDN) and so forth. The traffic is combined in the Firewall/Router then assigned to a VLAN according to the Access

Control List (ACL). This is called Traffic Filtering. The traffic then is assigned a priority using Quality of Service (QoS) for Traffic Prioritization. Then the traffic is sent to the Layer 3 Switch to be distributed to the necessary VLANs. DHS EINSTEIN enclave (1, 2,3a) for the participating traffic on VLANs and the internet for the non-participating traffic on a VLAN by itself. Once the participating traffic is returned from the DHS EINSTEIN enclave it is then sent out of the layer 3 switch which routes the traffic to the internet by VLAN to the Internet Circuit. The following diagram represents the use of redundant paths to ensure EINSTEIN enclaves remain operational in case of a network issue.

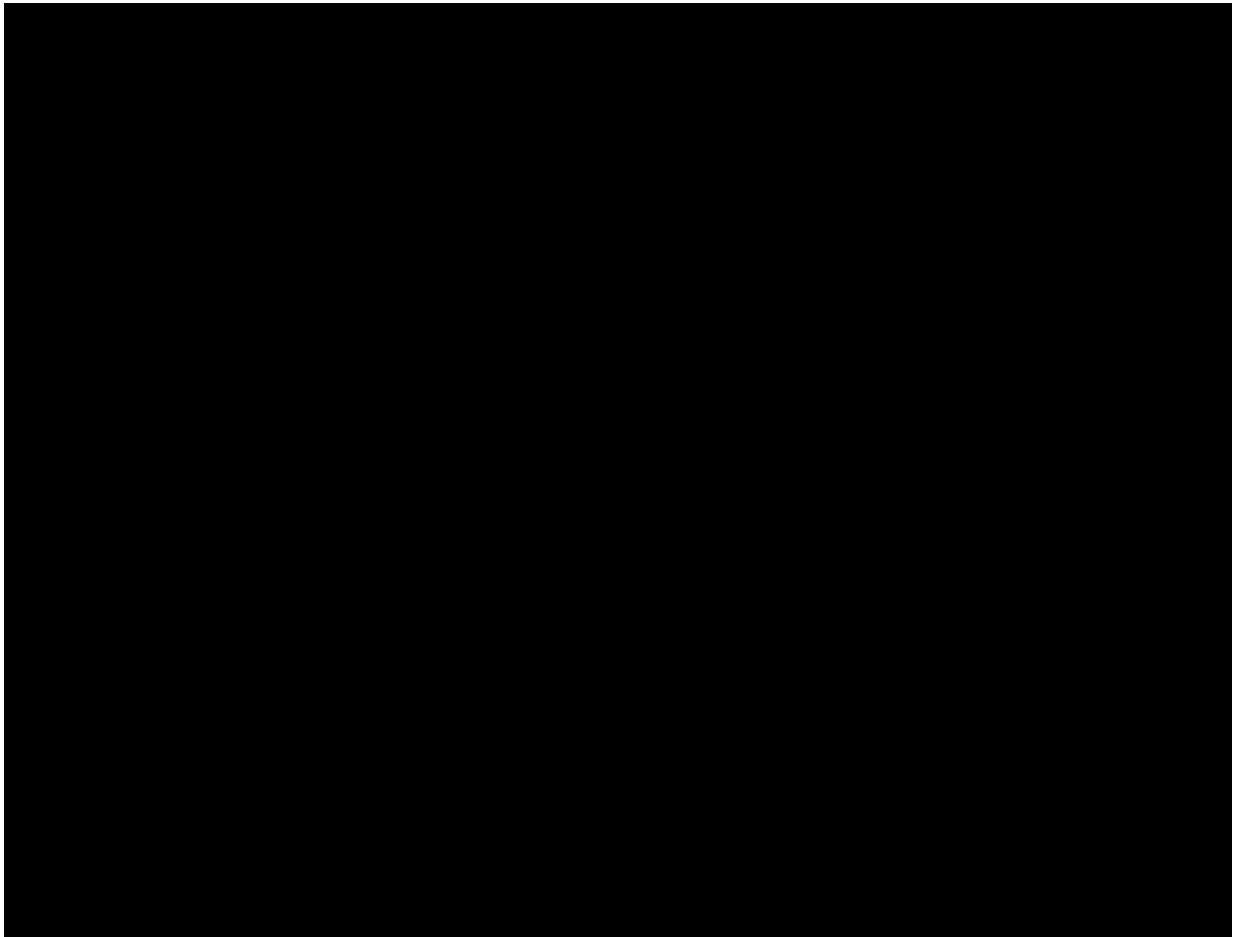


Figure 6: Redundant Paths Usage

The speed of the network equipment has the ability to handle 20Gps at the router and 10Gps at the switch. The Circuits available are at 100Mps, 1Gps, and 10Gps. These speeds are the most current at the present time.

Protocols Used and what Layer in the IOS they are used at:

Layer 1 Protocols - T-1 Pri, ISDN

Layer 2 Protocols - Frame Relay, Ethernet, VTP LAN Trunking, VLAN, MPLS (Layer 2.5)

Layer 3 Protocols – IPv4, IPsec, OSPF, RIP, EGP, GRE

Layer 4 Protocols – TCP, ESP

Layer 6 Protocol – TLS

Layer 7 Protocols – DNS, HTTP, HTTPS, IMAP, POP3, NTP, SMTP, SNMP

2.0 TECHNICAL RESPONSE (L.29.2)

2.1 EIS SERVICES (L.29.2.1) [RIN: MTC0013-DI]

2.1.1 EIS Scope for Mandatory Services (C.1.2)

2.1.1.1 Data Services (C.2.1)

2.1.1.1.1 Virtual Private Network Service (C.2.1.1) [RIN: MTR0131-DN]

CTI's Virtual Private Network Service (VPNS) will provide secure, reliable transport of agency applications across the provider's high-speed unified multi-service IP-enabled backbone infrastructure.

2.1.1.1.1.1 Service Description (C.2.1.1.1)

CTI's Virtual Private Network Service (VPNS) will provide secure, reliable transport of agency applications across the provider's high-speed unified multi-service IP-enabled backbone infrastructure. The CTI realizes VPNS are not perfect and limitations exist due to the many vendors the government may use at different agencies and differing technologies. However as the GSA EIS sets overall metrics, standards and performance goals, CTI will ensure government's needs are met and surpassed for any VPNS ordered. Since VPNS require detailed understanding of network security issues

and careful installation and configuration experience to ensure sufficient protection the CTI ensures this aspect of the service is accomplished professionally. CTI personnel are experts in resolving any type of compatibility issue brought about by the government's use of products and solutions from different vendors where compatibility issues arise due to VPN technology standards. Attempting to mix and match equipment may cause technical problems, and using equipment from multiple providers may not give the cost saving as expected. The CTI mitigates this potential problem by being familiar with all major vendors and product lines.

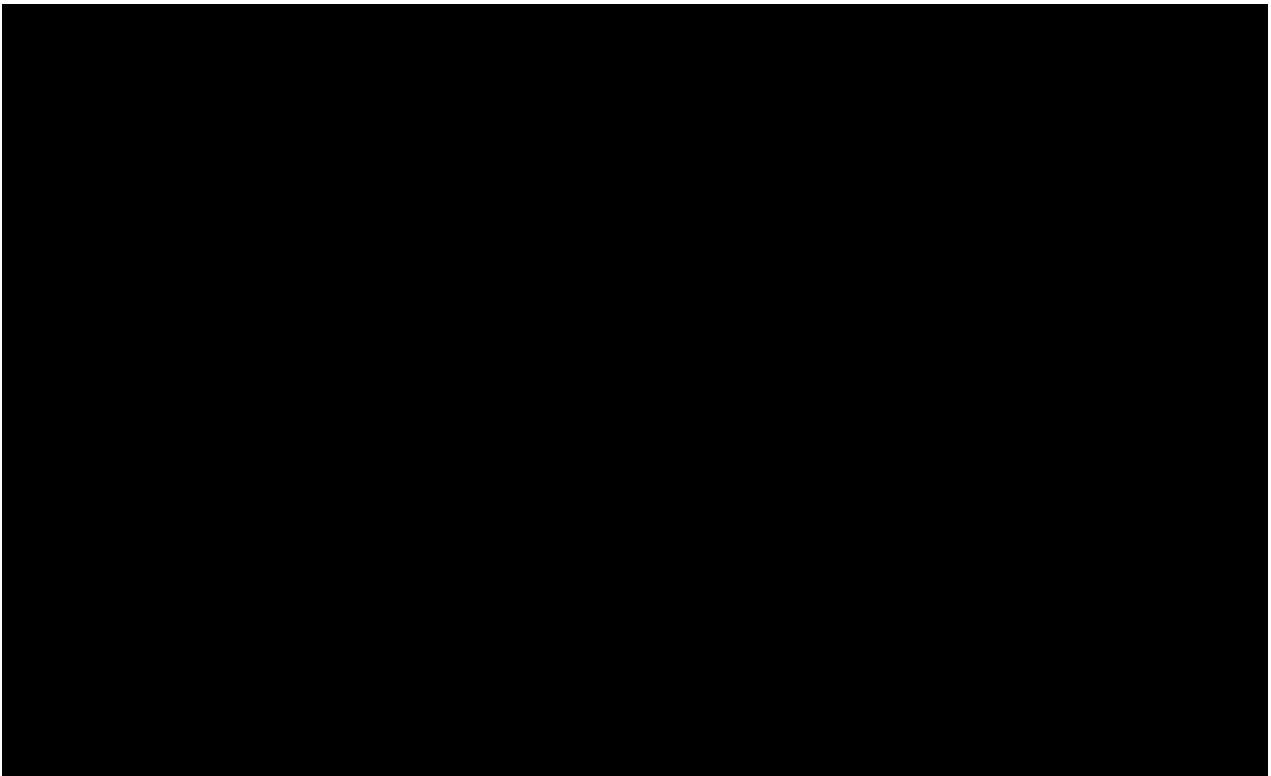


Figure 7: VPNS network diagram

2.1.1.1.1.1 Functional Definition (C.2.1.1.1.1)

The main characteristic of VPNS is that all infrastructure and devices involved in implementing the VPN are owned by the CTI and other vendors and located at the edge of our backbone. VPN tunnels terminate at CTI's edge router(s).

CTI will use our backbone to establish three basic solutions for VPNS:

1. Intranet – provides secure tunnels between remote sites, using broadband or dedicated access.
2. Extranet – enables trusted business partners to gain access to corporate information via secure/encrypted tunnels, using broadband or dedicated access.
3. Remote Access – enables mobile/remote workers to gain access to secure corporate information via secure encrypted tunnels, such as IPsec and SSL.

CTI will accommodate and optimize an agency's applications to enable the network to accurately and consistently allow for traffic prioritization and cost efficiencies.

Specifically, a VPN supports at least three different modes of use:

- Internet remote access client connections
- LAN-to-LAN internetworking
- Controlled access within an intranet

The CTI VPNS will support government critical needs such as:

4. Time-critical traffic such as voice and video.
5. Business-critical traffic such as transactions.
6. Non-critical traffic such as email.

CTI is aware that many security protocols have been developed as VPNs, each offering differing levels of security and features. Among the more common are:

- **IP security (IPSec):** IPSec is often used to secure Internet communications and can operate in two modes. Transport mode only encrypts the data packet message itself while Tunneling mode encrypts the entire data packet. This protocol can also be used in tandem with other protocols to increase their combined level of security.
- **Layer 2 Tunneling Protocol (L2TP)/IPsec:** The L2TP and IPsec protocols combine their best individual features to create a highly secure VPN client. Since L2TP isn't capable of encryption, it instead generates the tunnel while the IPsec protocol handles encryption, channel security, and data integrity checks to

ensure all of the packets have arrived and that the channel has not been compromised.

- **Secure Sockets Layer (SSL) and Transport Layer Security (TLS):** SSL and TLS are used extensively in the security of online retailers and service providers. These protocols operate using a handshake method. At the beginning of an SSL session, an SSL handshake is performed. This handshake produces the cryptographic parameters of the session." These parameters, typically digital certificates, are the means by which the two systems exchange encryption keys, authenticate the session, and create the secure connection.
- **Point-to-Point Tunneling Protocol (PPTP):** PPTP is a ubiquitous VPN protocol used since the mid-1990s and can be installed on a huge variety of operating systems. Like L2TP, PPTP doesn't do encryption; it simply tunnels and encapsulates the data packet. Instead, a secondary protocol such as GRE or TCP has to be used to handle the encryption. And while the level of security PPTP provides has been eclipsed by new methods, the protocol remains a strong one.
- **Secure Shell (SSH):** SSH creates both the VPN tunnel and the encryption that protects it. This allows users to transfer information unsecured data by routing the traffic from remote file servers through an encrypted channel. The data itself isn't encrypted but the channel it is moving through is. SSH connections are created by the SSH client, which forwards traffic from a local port one on the remote server. All data between the two ends of the tunnel flow through these specified ports. SSH is a technique that is used often to bypass government content filters. The CTI works with all types of VPN techniques and works to ensure these this type of VPN techniques is not used in cases where multiple provider are working on a single network/system.

2.1.1.1.1.2 Standards (C.2.1.1.1.2) [RIN: MTC0002-DI]

The CTI VPNS will comply with all the following standards.

1. OMB M-11-11 “Continued Implementation of Homeland Security Presidential Directive (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors”
2. NIST Special Publication (SP) 800-46 Revision 1 “Guide to Enterprise Telework and Remote Access Security”
3. IETF RFCs:
 1. For secure VPNs:
 - i. General IPSec
 - ii. ESP and AH
 - iii. Key exchange
 - iv. Cryptographic algorithms to include but not limited to 3DES, RC4 and AES
 - v. IPSec policy handling
 - vi. IPSec MIBs
 - vii. Remote access
 - viii. Certification Authorities
 2. For trusted VPNs:
 - i. General MPLS
4. IP Security Working Group – RFC 4303
5. IP Security Policy Working Group – RFC 3586
6. MPLS Working Group – RFC 3468
7. Layer 3 Virtual Private Network (L3VPN) Working Group – RFC 4176
8. Pseudo Wire Emulation Edge to Edge (pwe3) Working Group – RFC 3985
9. Use of PE-PE GRE or RFC4364 VPNs:
10. IETF-TLS Working Group – RFC 5246 for TLS 1.2
11. TLS 1.2 Protocol Specification
12. IETF RFCs for IPv4 and IPv6
13. CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information Among National Security Systems

14. All new versions, amendments, and modifications to the above documents and standards

2.1.1.1.1.3 Connectivity (C.2.1.1.1.3)

The CTI VPNS will connect government locations and trusted business partners via leased lines for site-to-site access or broadband for remote access to provide direct connectivity between all sites as a partially- or fully-meshed WAN. The CTI VPNs, allow users to securely access a private network and share data remotely through public networks. Much like a firewall protects data on a computer, VPNs protect it online. A VPN is *technically* a WAN (Wide Area Network), however the front end retains the same functionality, security, and appearance as it would on a private network.

2.1.1.1.1.4 Technical Capabilities (C.2.1.1.1.4) [RIN: MTR0010-DN]

CTI assumes the following VPNS capabilities are mandatory unless marked optional.

1. CTI will meet applicable routing requirements in the GSA EIS solicitation Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.
2. CTI will provide multiple tunneling standards, as required by an agency. Examples include L2TP, GRE, IP-in-IP, MPLS, IPSec, and SSL/TLS.
3. CTI will provide various encryption levels, as required by an agency. Examples include 3DES, RC4 and AES in accordance with the appropriate FIPS publications and modules.
4. CTI will provide authentication services as required by an agency. Examples include RADIUS, Internal LDAP, token integration, PKI, and X.509 certificates.
5. CTI will support IPv4 as both the encapsulating and encapsulated protocol.
6. CTI will support IPv6 as both the encapsulating and encapsulated protocol.
7. CTI will support QoS in the following standardized modes:
 - a. Best effort

-
- b. Aggregate Customer Edge (CE) Interface level QoS (“hose” level)
 - c. Site-to-site level QoS (“pipe” level)
 - d. Intserv (RSVP) signaled
 - e. Diffserv marked
 8. CTI will support QoS across a subset of the access networks as listed below:
 - a. 802.1p Prioritized Ethernet
 - b. MPLS-based access
 - c. Multilink Multiclass PPP
 - d. QoS-enabled wireless:
 - i. LTE
 - ii. Wireless 802.11.x
 - iii. Cable high-speed access (DOCSIS 1.1)
 - iv. QoS-enabled Digital Subscriber Line (DSL)
 - v. QoS-enabled Satellite Broadband Access
 9. CTI will support one or more of the following application level QoS objectives:
 - a. Intserv model for selected individual flows
 - b. Diffserv model for aggregated flows
 10. CTI will provide isolation of traffic and routing service that isolates the exchange of traffic and routing information to only those sites that are authenticated and authorized members of a VPN. CTI will provide layered security architecture to ensure that attackers will not find a single point of entry but will be faced with multiple levels of security.
 11. CTI will support multiple VPNs by allowing both permanent and temporary access to one or more VPNs for authenticated users across a broad range of access technologies using a variety of COTS products that meet the specific need of government customers.
 12. CTI will provide secure routing services to provide full routing capability on the VPN platform with a secure policy across the VPN.
-

13. CTI will support the inclusion of encryption, decryption, and key management profiles as part of the security management system. Please see the section titled, "Managed Security Services" section 2.1.3.8.7 of this document.
14. CTI will support an agency in deploying its own internal security mechanisms in addition to those deployed by CTI, in order to secure specific applications or traffic at a granularity finer than a site-to-site basis.
15. CTI will allow an agency to choose from alternatives for authentication of temporary access users so long as the authentication alternative meets government standards as outlined within the GSA EIS solicitation. Authentication server choices include:
 - a. Contractor-provided
 - b. Third party
 - c. Agency-provided

CTI will meet or exceed each of the technical capabilities as specified for VPNs. CTI will meet each of the listed Key Performance Indicators (KPIs) and if applicable will exceed the stated KPIs, where possible.

Quality of Service (QoS) for networks is an industry-wide set of standards and mechanisms for ensuring high-quality performance for critical applications. CTI will use QoS mechanisms to prioritize, and manage the network traffic. The use of these mechanisms ensures that resources are used efficiently to provide the required level of Quality of Service.

Some measurements for QoS are (but not limited to):

1. Bandwidth - one of the most critical criterion for QoS. It is basically the size of the data or packet load carrying capability. A network experiences congestion when it is presented with more traffic than it can handle, therefore adequate bandwidth is critical in maintaining QoS.
2. Packet loss - Percentage of packets which did not arrive correctly •
 - a. Limits: – At most: 1% for voice packets and 2% for video – Desired: 0%

3. Latency - Time a packet takes to go from the source’s outgoing interface to the destination’s incoming interface •
 - a. Limits: – At most: 150 ms – Desired: 0 ms.
4. Policies - traffic policy rules match defined conditions and start specific actions. The traffic policy rules define the necessary criteria that must be met in order for the rule's actions to be applied. These will be applied where appropriate.
5. Jitter • Latency variation among received packets •
 - a. Limits: – At most: 50 ms average difference between packets – Desirable: as less as possible.

Some Basic Key Performance Indicators that must be monitored:

CTI shall monitor their customers’ network for three basic key performance indicators (KPIs):

- *Availability* is the measure of the “reachability” or accessibility of one measurement point from another measurement point at the network layer. The underlying routing and transport infrastructure of the provider network will support the availability measurements, with failures highlighted as unavailability.
- *Health* measures the number and type of errors that are occurring on the customer network, and can consist of both router-centric and network-centric measurements, such as hardware failures or packet loss.
- *Performance* of the customer network measures how well it can support IP services (for example, in terms of delay or utilization).

2.1.1.1.1.2Features (C.2.1.1.2)

CTI assumes the following VPNS features are mandatory unless declared optional by the government.

ID Number	Name of Feature	Description
1	High availability options for CPE	CTI will provide the following high availability options: <ol style="list-style-type: none"> 1. Fault tolerance 2. Load sharing 3. Fail-over protection 4. Diverse access points to service provider’s POP(s).

2	Interworking Services	CTI will provide interworking services for an agency's VPN to transparently access agency locations that use CTI's Ethernet Service.
---	-----------------------	--------------------------------------------------------------------------------------------------------------------------------------

Table 1: VPNS Features table (C.2.1.1.2)

2.1.1.1.1.3 Interfaces (C.2.1.1.3) [RIN: MTR0106-DN, MTR0005-DN]

CTI will support the interfaces as stated below for its VPNS offering.

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type (See Note 1)
1	Ethernet Interface	1 Mbps up to 10/40/100 Gbps (Std IEEE802.3ae and 802.3ab)	IPv4/v6 over Ethernet
2	Private Line Service	<ol style="list-style-type: none"> 1. DS0 2. T1 3. T3 4. OC-3c 5. OC-12c 6. OC-48c 7. OC-192c 8. OC-768c 	IPv4/v6 over PLS
3	IP over SONET Service	<ol style="list-style-type: none"> 1. OC-3c 2. OC-12c 3. OC-48c 4. OC-192c 5. OC-768c 	IP/PPP over SONET
4	DSL Service	xDSL access at 1.5 to 6 Mbps uplink, and 384 Kbps to 50 Mbps downlink	Point-to-Point Protocol, IPv4/v6
5	Cable high speed access	256 Kbps up to 150 Mbps (Standard DOCSIS 3.0)	Point-to-Point Protocol, IPv4/v6
6	Wireless Access	<ol style="list-style-type: none"> 1. Wi-Fi 2. LTE 3. Satellite 	Point-to-Point Protocol, IPv4/v6

Table 2: VPNS Interfaces table (C.2.1.1.3)

Notes:

1. IPv6 will be supported by CTI
2. Where E-1/E-3 carrier service is provided, appropriate corresponding payload data rates apply.

2.1.1.1.1.4 Performance Metrics (C.2.1.1.4) [RIN: MTR0006-DN]

CTI will meet each of the KPIs as stated below for its VPNS offering.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Latency (CONUS)	Routine	70 ms	≤ 70 ms	See Note 1
Latency (OCONUS)	Routine	150 ms	≤ 150 ms	See Note 2
Av(VPN)	Routine	99.9%	≥ 99.9%	See Note 3
	Critical	99.99%	≥ 99.99%	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	See Note 4
	With Dispatch	8 hours	≤ 8 hours	

Table 3: VPNS Performance Metrics table (C.2.1.1.4)

Notes:

1. Latency value is the average round trip transmission between agency premises routers for a VPN with all of its CONUS sites. Latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods. Relevant standards are RFC 1242 and RFC 2285. CTI may propose to the government more cost-effective test and measurement technique alternatives that meet or exceed the requirements in RFC 1242 and RFC 2285.
2. Latency value is the average round trip transmission between agency premises routers for an IP VPN with its CONUS and OCONUS sites. Latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods. Relevant standards are RFC 1242 and RFC 2285. CTI may propose to the government more cost-effective test and measurement technique alternatives that meet or exceed the requirements in RFC 1242 and RFC 2285.
3. VPN availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the VPN is operationally available to the agency.
4. See Section G.8.2.1.2 for the definitions and measurement guidelines.

2.1.1.1.2 Ethernet Transport Service (C.2.1.2)

2.1.1.1.2.1 Service Description (C.2.1.2.1)

CTI provides carrier grade Ethernet transport service, implemented over an MPLS backbone, where Ethernet links are transported using MPLS label switched paths (LSPs) inside an outer MPLS “tunnel.” This strategy supports point-to-point and

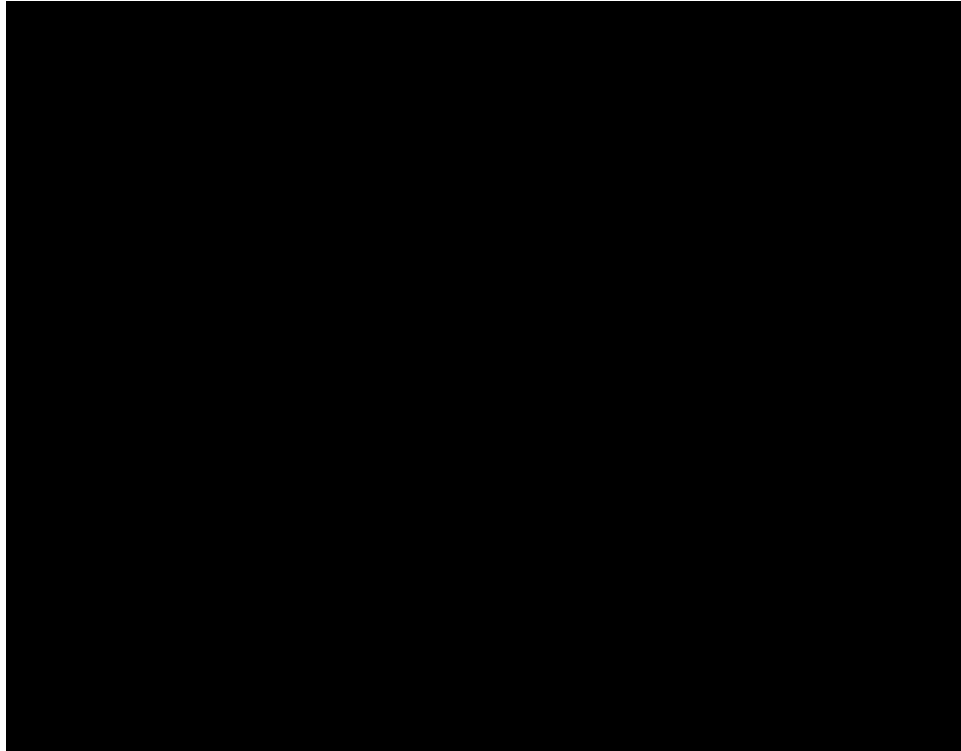


Figure 8: ETS network diagram

multipoint services, and has achieved significant deployment in routed networks. Ethernet Transport Service (ETS) allows agencies to interconnect their LANs (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 Gbps) transparently over the Metro Area Networks (MAN) and the Wide Area Networks (WAN), regardless of the geographical location of their sites. Ethernet Transport Service enables Intranet and Extranet services, as well as intra- and inter-agency communications.

[Redacted text block consisting of four horizontal black bars]

Dedicated Ethernet is defined as private services that are carried over dedicated facilities at fixed and predetermined speeds. Shared Ethernet is defined as statistically multiplexed Ethernet connections.

2.1.1.1.2.1.1 Functional Definition (C.2.1.2.1.1)

CTI satisfies the Government's requested capabilities for Ethernet services by offering Virtual Private LAN Service (VPLS) and Virtual Private Wire Service (VPWS), which represent advanced packet-switched VPN solutions that blend Layer 2 and Layer 3 technologies to make it possible to operate private, point-to-point, and multipoint virtual LANs through public networks.

Our Ethernet Transport Services (ETS) exploits Ethernet's flexibility, cost effectiveness, and differentiation of service (e.g., traffic priority) capabilities while providing end-to-end transport of data traffic with minimal protocol conversion. The following ETS shall be supported:

1. Ethernet Private Line (E-LINE). E-Line is a point-to-point service in which bandwidth is reserved. E-Line supports full port speeds (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 or higher Gbps) and can support different quality of service (QoS) priorities for customer traffic. E-Line is a point-to-point configuration as a Layer 2 tunnel that provides a transparent, dedicated connection between two sites. This service resembles/replaces traditional Time Division Multiplexing (TDM) private line service. Some applications include router interconnect, business continuity, and disaster recovery. E-LINE service can be offered over the MAN and/or WAN.
2. Ethernet Private LAN (E-LAN). E-LAN supports both point-to-multipoint and multipoint-to-multipoint configurations. For point-to-multipoint configurations, ETS connects three or more sites over Layer 2 tunnels. It supports full port speeds (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 or higher Gbps) and can support different Quality of Service (QoS) priorities for customer traffic. For multipoint-to-multipoint configuration, also called E-Tree service, ETS connects

several sites (similar to point-to-multipoint configuration) by connecting one or more roots and a set of leaves, but preventing inter-leaf communication. More than one site can be configured, as the root site and other sites can communicate with each other through multiple root sites; for example, connecting disparate LAN segments into a single agency-wide virtual LAN. E-LAN can be offered over the MAN and/or WAN.

2.1.1.1.2.1.2 Standards (C.2.1.2.1.2)

CTI ETS will ensure and comply with the following standards in providing ETS:

Metro Ethernet Forum (MEF CE 2.0):

1. (Optional) Support Jumbo Ethernet frames
2. CE 2.0 is set of MEF CE 2.0 Certified network elements that connect to transport Carrier Ethernet services for all users, locally and worldwide. Ethernet transport services are carried over physical Ethernet networks and other legacy transport technologies.
3. Key Specifications:
 - MEF 6.1 - CE Service Definitions
 - MEF 10.2 - CE Service Attributes
 - MEF 33 - Ethernet Access Services
 - MEF 23.1 - Class of Service
 - MEF 26.1 - ENNI
 - CE 2.0 expands CE 1.0 to:
 - 8 services, 2 of each respectively in E-Line, E-LAN, E-Tree, and E-Access (defined in MEF Standards MEF 6.1, 22.1, 33).
 - Standardized Multi-CoS with application-oriented CoS Performance Objectives, new metrics (MEF 6.1, 10.2, 20, 23.1).
 - Interconnect through the integrated delivery of MEF Service Attributes (MEF 10.2, 26.1, 33) allows ubiquitous deployment spanning multiple providers.
 - Manageability, (MEF 7.1, 16, 17, 30, 31) plus additional specifications.

3. International Telecommunications Union (ITU):

a) Network architecture:

- G.8010/Y.1306 Architecture of Ethernet layer networks

b) Services:

- G.8011/Y.1307 Ethernet over Transport – Ethernet services framework
- G.8011.1/Y.1307.1 Ethernet private line service
- G.8011.2/Y.1307.2 Ethernet virtual private line service
- G.8011.3/Y.1307.3 Ethernet virtual private LAN service (draft)
- G.8011.4/Y.1307.4 Ethernet virtual private rooted multipoint service (draft)
- G.8012/Y.1308 Ethernet UNI and Ethernet NNI

c) OAM:

- Y.1730 Requirements for OAM functions in Ethernet-based networks and Ethernet services
- Y.1731 OAM functions and mechanisms for Ethernet-based networks

d) Protection:

- G.8031/Y.1342 Ethernet linear protection switching
- G.8032/Y.1344 Ethernet ring protection switching

e) Equipment:

- G.8021/Y.1341 Characteristics of Ethernet transport network equipment functional blocks

f) Equipment management:

- G.8051/Y.1345 Management aspects of the Ethernet-over-Transport (EoT) capable network element

g) Terminology:

- G.8001/Y.1354 Terms and definitions for Ethernet frames over Transport (EoT)

4. Institute of Electrical and Electronics Engineers, Inc. (IEEE):

- IEEE 802.3, 1Gbps LAN PHY, 10Gbps LAN PHY, 10Gbps WAN PHY
- IEEE 802.3ae, 10Gbit Ethernet 802.17, Resilient Packet Rings (RPR) – in progress
- IEEE 802.1ah, Ethernet First Mile
- IEEE 802.1p
- IEEE 802.1q

5. Acceptance Testing of ETS:

- RFC 2544
- RFC 6815

6. All new versions, amendments, and modifications to the above documents and standards

2.1.1.1.2.1.3 Connectivity (C.2.1.2.1.3)

CTI ETS shall connect to and interoperate with:

- Intra-agency LAN-LAN Connectivity. ETS provides connectivity for an agency's LANs located in the same city or different cities, thereby extending the LAN to the MAN and WAN. This is achieved by connecting the agency's SDP(s) in one location to another SDP(s) in one or more locations. Interconnection shall be possible over transoceanic links, if required.
- Inter-agency LAN-LAN Connectivity. Different agencies may share resources to connect to the contractor's metro or long haul network. This is achieved by connecting from one agency's SDP(s) to other agencies' SDP(s).

2.1.1.1.2.1.1 Technical Capabilities (C.2.1.2.1.4) [RIN: MTR0113-DN, MTR2244-DN, MTC0003-DI]

CTI understands the following ETS capabilities are mandatory unless marked optional:

1. CTI will meet applicable routing requirements in the GSA EIS solicitation, ensuring any encrypted tunnels are applied and proxied to allow inspection.
2. Geographical Coverage. CTI will provide a seamless end-to-end service from the SDP Customer Premise Equipment (CPE) traversing CTI's network (Metro Access/Core and Long Haul) in order to minimize conversion of protocols. CTI will indicate if protocol conversions are required and how they impact the delay when delivering end-to-end services. The following geographical coverage shall be provided:
 - a. Intra-City ETS – CTI will provide Ethernet connections to agency sites located within the same city both inside the US (CONUS and Metro) and outside the US (OCONUS and Non-Domestic).
 - b. Inter-City ETS – CTI will deliver Ethernet connections at domestic and non-domestic locations (CONUS/Metro, OCONUS/Non-Domestic).

3. CTI will support Ethernet UNI (User-to-Network-Interface) to support Layer 2 and Layer 3 clients. Layer 3 clients are agency devices that support Layer 3 protocol packets such as IPv4, IPv6.
4. CTI will support Ethernet Virtual Connections (EVCs).
5. CTI will support delivery of the ETS at the agency's Service Delivery Point (SDP) via a UNI.
6. CTI will support circuit emulation services for TDM services, when required.
7. CTI will support point-to-point, multi-point-to-multi-point, and point-to-multi-point EVCs.
8. CTI will support EVC multiplexing.
9. CTI will support rate-limited throughput access links, i.e., 1 Gbps port rate limited in 100 Mbps increments.
10. CTI will support rate-limiting at the agency's SDP and at the individual VLAN ingress and egress.
11. CTI will support privacy and security per IEEE 802.3 as defined in the TO.
12. CTI will support the following service attributes:
 - a. CTI will support physical interfaces as listed in Section 2.1.1.1.2.3.
13. CTI will support the following traffic profiles:
 - a. Committed Information Rate (CIR) – minimum amount of bandwidth guaranteed for an ETS
 - b. Committed Burst Size (CBS) – the size up to which subscriber traffic is allowed to burst and still be in-profile and not discarded or shaped
 - c. Peak Information Rate (PIR) – specifies the rate above the CIR that traffic is allowed into the network for a given burst interval defined by the MBS
 - d. Maximum Burst Size (MBS)
14. Performance parameters shall be supported as listed in Section 2.1.1.1.2.4.
15. CTI will support Service Frame Delivery options to include:
 - a. Unicast Frame Delivery
 - b. Multicast Frame Delivery, as per RFC 4604
 - c. Broadcast Frame Delivery as per IEEE 802.3
16. VLAN tag supported shall include:
 - a. VLAN tag preservation

-
- b. VLAN tag translation
 - c. VLAN tag stacking
 - d. VLAN aggregation across a common physical connection (optional)
17. CTI will support multiplexing to include multiple EVCs connected via a single UNI.
18. Bundling shall be supported to enable two or more VLAN IDs to be mapped into a single EVC at a UNI.
19. Security Filters shall be supported as specified in the TO.
20. (Optional) CTI will provide proactive Performance Monitoring (PM) and support the following:
- a. Signal failure
 - b. Signal degradation
 - c. Connectivity or Loss of connectivity
 - d. Frame loss
 - e. Errored frames
 - f. Looping
 - g. Denial of service (DoS)
 - h. Mis-inserted frames
 - i. Maintenance parameters
21. CTI will support the following maintenance functions:
- a. Alarm suppression
 - b. Loopbacks [intrusive and non-intrusive (transparent to on-going connections)]
 - c. Protection switching, restoration, etc.
22. CTI will support the following network topologies:
- a. Point-to-point
 - b. Rooted Multipoint
 - c. Multi-point-to-Multi-point (i.e., mesh)
23. CTI will support geographical diversity to provide added reliability. An agency may buy a geographical diverse route from the same or a different contractor to serve as a protection path.

-
24. CTI will support bridging in compliance with IEEE 802.1Q.
 25. CTI will support the following Virtual Connection sizes:
 - a. For point-to-point Ethernet connections – up to 40 Gbps
 - b. For multi-point-to-multi-point connections – up to 40 Gbps
 26. Quality of Service (QoS) – CTI will support traffic prioritization that enables higher priority traffic to be transmitted first.
 27. CTI will support traffic reconfiguration that supports the ability of the agency to modify a specific service connection subsequent to the establishment of the connection. Changes to an established connection may include upgrade/downgrade of speeds that do not result in physical equipment changes.

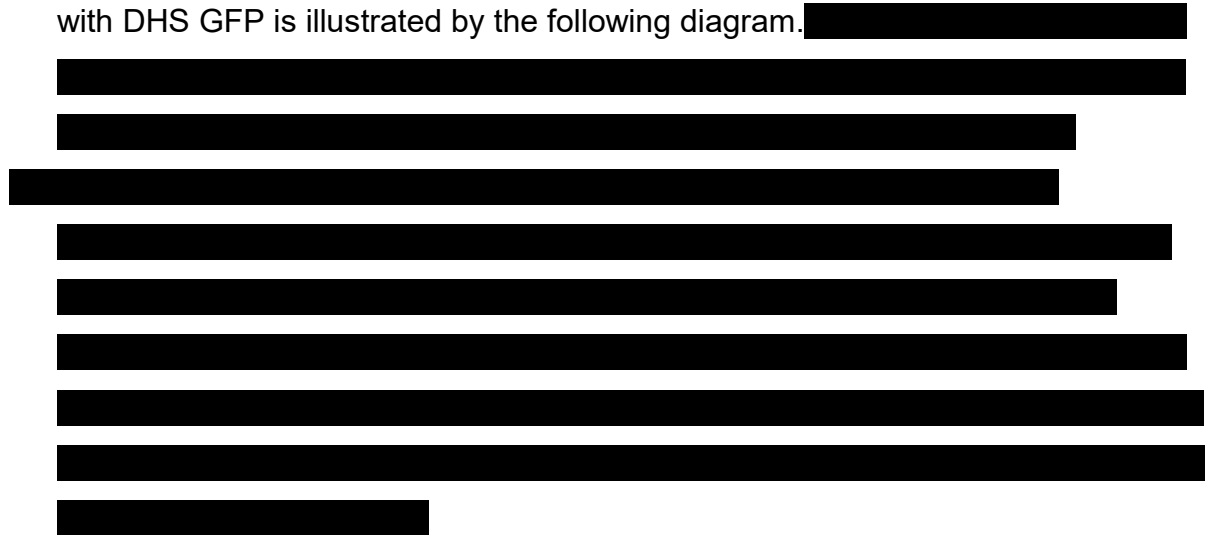
CTI meets the external traffic routing requirements described in Section C.1.8.8, subparagraph 3, which include:

1. CTI's methodology for identifying the offeror's participating agency traffic for each affected service shall be via IP addresses. Participating agency traffic network traffic is defined by the list of IP addresses and non-IP sources supplied by each agency and verified by DHS. Any non-IP sources shall be converted to IPs so they can be routed over the network.
2. CTI's anticipated technical approach for each affected service, to redirect all participating agency Internet, Extranet, and inter-agency traffic to DHS EINSTEIN enclaves, is to receive processed traffic from GFP within the DHS EINSTEIN enclave and deliver that traffic to its final destination via VLAN routing. Using VLAN routing and Access Control Lists (ACLs), all incoming participating traffic is tagged with VLANs to be redirected to EINSTEIN Enclaves. All traffic received from the EINSTEIN enclave is forwarded to its final destination.
3. CTI's technical approach to notify DHS should any non-participating agency traffic (IPv4, IPv6, etc.) be redirected through DHS EINSTEIN enclaves is via email and trouble reporting and ticket tracking tools. Currently CTI uses Remedy 9 Enterprise to support our Navy customers. In our experience this is the most often used interface between customer and MNS provider. Remedy uses Smart

Reporting which is an easy way to provide visual insight into what is happening within the network.

4. Control mechanisms that CTI shall use to ensure that the identification and redirection of participating agency traffic is not inadvertently or maliciously bypassable shall be accomplished on CTI's network prior to purchase and deployment. Testing shall cover voice, data, and video technologies that include but are not limited to, IP VPN and voice services. Testing shall be performed at the agency's discretion and structured in collaboration with CTI, either at CTI's headquarters or with the appropriate CTI partner depending upon type and classification of network tested. CTI will create testing environments to include sufficient equipment, software and licenses in order to replicate voice, data, video technologies and services that will be supplied to the government. Within this test environment, CTI will be able to check equipment capability, interoperability, delivery of services, and compare, prior to any delivery, any baseline changes. Baseline changes deemed to have an impact on operations, or to have an adverse effect on performance will be applied, and the unit tested on a development rack, then merged onto an integration test rack; performance tested then delivered for installation.

Sensing and control mechanisms CTI will use to ensure the redirection of traffic is failsafe (no disruption of participating agency services) should failures occur with DHS GFP is illustrated by the following diagram.



[REDACTED]

7. CTI shall provide instrumentation to measure transport SLA KPIs (as if traffic passes through loopbacks in EINSTEIN Enclaves with no impact within DHS GFP being counted against the CTI's performance) by using Network Monitoring Service tools [REDACTED].

[REDACTED]

- Cisco NBAR support – advanced application recognition to identify which applications, categories, and subcategories consume the most bandwidth for better visibility into network traffic with NBAR2 support
- Customizable network traffic reports to create, schedule, and deliver in-depth network traffic and bandwidth reports with just a few clicks.
- Integrated fault, performance, and configuration management to seamlessly integrate with Network Performance Monitor and Network Configuration Manager
- Wireless LAN Controller traffic monitoring for WLC traffic to see which applications and clients utilize the bandwidth of your wireless network.

2.1.1.1.2.2 Features (C.2.1.2.2) [RIN: MTR0069-DN]

Reserved.

2.1.1.1.2.3 Interfaces (C.2.1.2.3)

CTI will provide UNIs at the SDP unless marked optional:

UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling Protocol Type/Granularity
1	Optical	IEEE 802.3z	1310 nm	1.25 Gbps	Gigabit Ethernet
2	Optical	IEEE 802.3z	850 nm	1.25 Gbps	Gigabit Ethernet
3 (optional)	Optical	IEEE 802.3	1310 nm	100 Mbps	Fast Ethernet
4 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm	10/40/100 Gbps	10/40/100GBASE-SR (65 meters)
5 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	850nm	10/40/100 Gbps	10/40/100GBASE-SW
6 (optional)	Optical	IEEE 802.3ae	1550 nm	10/40/100 Gbps	10/40/100GBASE-ER

		IEEE 802.3ba			
7 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm	10/40/100 Gbps	10/40/100GBASE- LR
8 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1550 nm	10/40/100 Gbps	10/40/100GBASE- LW
9 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1300 nm Multimode	10/40/100 Gbps	CWDM 10/40/100GBASE- LX4 (300 meters)
10 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm Single Mode	10/40/100 Gbps	CWDM 10/40/100GBASE- LX4 (10,000 meters)
11 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm Single Mode	10/40/100 Gbps	10/40/100GBASE- LW (10,000 meters)
12 (optional)	Optical	IEEE 802.3ae IEEE 802.3ba	1550 nm Single Mode	10/40/100 Gbps	10/40/100GBASE- EW (40,000 meters)
13 (optional)	Electrical	IEEE 802.3	N/A	10 Mbps	10Base
14	Electrical	IEEE 802.3	N/A	100 Mbps	100 Base
15	Optical	IEEE 802.3		1 Gbps	1000Base
16 (optional)	Optical	ITU-T G.707	1300 nm	STM-4	SDH STM-1, VC-11 (DS1), VC-12 (E1), VC-3 (DS3, E3, other), VC-4

17 (optional)	Optical	ITU- G.707	1300 nm	STM-4c	VC-4-4c
18	Optical	IEEE 802.3z IEEE 802.3ab	Multimode	1 Gbps	1000BASE-LX
19	Optical	IEEE 802.3z IEEE 802.3ab	Multimode	1 Gbps	1000BASE-SX
20 (optional)	Electrical (Copper)	IEEE 802.3z	N/A	1 Gbps	1000BASE-CX
21 (optional)	Electrical (Twisted pair)	IEEE 802.3z	N/A	1 Gbps	1000BASE-T
22 (optional)	Optical	GR-253, ITU- T G.707	1310 nm	10/40 Gbps	SONET or SDH

Table 4: ETS Interfaces table (C.2.1.2.3)

2.1.1.1.2.4 Performance Metrics (C.2.1.2.4) [RIN: MTC0005-DI]

CTI offers Agencies Ethernet Services that meet or exceed the performance standards of the government defined KPI's. The proposed service quality levels represent the minimum level of service that Agencies will be provided. Focusing on an Agency's service experience produces a high-quality solution, and service experience must be measured quantitatively through the KPIs. However, high quality is not necessarily attained through exceptional performance of a single KPI. For example, an inferior response to the Agencies' maintenance and support needs can quickly erase the benefits of exceptional network latency performance. Agencies will receive high-quality service through the combination of the six network and service attributes that directly affect the quality delivered to the end user: scale, global footprint, high availability, and data delivery, low-packet latencies, and quick-service restoration.

CTI will meet the performance levels and AQL of KPIs for ETS unless marked optional:

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Av (ETS)	Routine	99.9%	≥ 99.9%	See Note 1

	(Single Connection)			
	Critical (Double Connection)	99.99%	≥ 99.99%	
Latency (ETS)	CONUS	100 ms	≤ 100 ms	See Note 2
	OCONUS	200 ms	≤ 200 ms	
Jitter (Packet)	Routine	10 ms	≤ 10 ms	See Note 3
Grade of Service (Packet Delivery Rate)	Routine	99.95%	≥ 99.95% at all times	See Note 4
	Critical	99.99%	≥ 99.99% at all times	
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	See Note 5
	With Dispatch	8 hours	≤ 8 hours	
Grade of Service (Fail Over Time)	Routine	1 minute	1 minute	See Note 6
	Critical	100 ms	≤ 100 ms	See Note 6

Table 5: ETS Performance Metrics table

Notes:

- CTI understands ETS availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the ETS is operationally available to the agency. Availability is computed by the standard formula:

$$Av(EthS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

- CTI understands that Latency is the round trip delay experienced by an end user across the contractor's network to other agencies' sites. It is the average time for packets to travel over the CTI network. The Internet Control Message Protocol (ICMP) test can be used to calculate packet delivery and latency. The ICMP test consists of sending, every five minutes, a series of five test packets between originating agency's SDPs and the delivery SDPs. The test results are analyzed to determine packet loss vs. successful delivery and speed of delivery. Contractor shall meet or exceed standards set by RFC 1242 and RFC 2285. It can be determined by the following formula: $(\text{Distance}/(0.6*c)+\text{hops}*\text{delay})$, where c is the velocity of light and 0.6 is the multiplier recommended by the ITU (G.144) in ms/km plus the delay in each hop caused by the routers times the number of hops.
- CTI understands that measurements of packet jitter are performed by injecting packets at regular intervals into the network and measuring the variability in the arrival time. Relevant standard is RFC 2679.
- CTI understands that network devices, such as switches and routers, sometimes have to hold data packets in buffered queues when a link gets congested. If the link remains congested for too long, the buffered queues will overflow and data will be lost. The loss can be measured with the ICMP test. CTI will meet or exceed relevant standards such as RFC 1242 and RFC 2285.
- CTI understands that restoration for links transported over the Ethernet infrastructure (i.e., Ethernet switches) is achieved by the use of protocols such as Spanning Tree (IEEE 802.1d), which converge more slowly than SONET. Therefore, ETS for critical users shall be delivered over a carrier class infrastructure.

2.1.1.2 Voice Service (C.2.2)

CTI's Voice Service (VS) is a service comprised of voice circuits typically capable of carrying one telephone conversation or its digital equivalent. Within the USA ,analog voice circuits have been replaced with digital equivalent circuits with a 64 kbps standard

for both Time Division Multiplex (TDM) and Internet Protocol (IP) based backbone circuits. VS supports outgoing voice calls by direct station-to-station dialing from on-net and off-net locations worldwide, including calling cards.

VS calls can be initiated from many types of telephony equipment, including single-line and multi-line key sets. VS calls typically traverse trunks to PBX and Centrex equipment and terminate in a variety of telephony equipment, which may include secure telephone units and connection to Inmarsat mobile satellite devices.

CTI VS are provided using various technologies for GSA EIS and are organized as:

1. Internet Protocol Voice Service (IPVS)
2. Circuit Switched Voice Service (CSVS)

CTI will provide both of the VS technologies specified above, with IPVS as its mandatory VS solution and CSVS as its optional.

2.1.1.2.1 Internet Protocol Voice Service (C.2.2.1)

Internet Protocol Voice Service (IPVS) provides voice communications service and telephony features to agencies using IPVS over a managed IP network. IPVS is an enterprise solution that consolidates a subscriber's voice and data traffic over a single data network and enables agencies to manage their network more efficiently, while reducing costs and taking advantage of new, leading-edge, multimedia business capabilities.

2.1.1.2.1.1 Service Description (C.2.2.1.1) [RIN: MTC0014-DI]

CTI's IPVS is a network-based (hosted) and premises-based telephone service over the CTI-provided IP network. CTI can provide a Managed LAN Service and Session Initiation Protocol (SIP) Trunking Service in accordance with government request.

CTI's IPVS capability is a fully managed service using Cloud based IPVS technology over an IP network. It offers end users cost savings and improved efficiency. CTI offers

both a Hosted Voice service and SIP Trunking – these services can operate independently or as a cooperative package across sites.

Hosted Voice– An option available for agencies that do not have a PBX on site but use a virtual PBX facility. Hosted Voice offers a resilient Cloud hosted service that is not affected by physical or geographic inhibitors that may otherwise affect a locally hosted service, which reduces outages and down time.

Premises Based - CTI will provide a premise-based systems are solutions where the equipment - including phone system servers, cabling and routers - are installed and maintained locally. This high level of support helps ensure system hardware and applications are constantly updated to meet the emerging needs of the marketplace.

A premise-based system(s) can be digital, VoIP or a hybrid. While many agencies and companies want to take advantage of the collaboration, productivity, and mobility solutions VoIP offers, hybrid Digital/VoIP systems ([REDACTED]) offer a phased migration path to VoIP for agencies or companies without the financial or personnel resources to make the transition all at once. Premise-based systems are such that the hardware is owned by the customer. This can be beneficial for the government if their IT upgrade budgets and/or sizable dedicated internal IT staff. These systems can either be serviced by the provider via a maintenance contract or internally by the company's IT staff.

SIP Trunking– An option for agencies that have their own PBX on site with calls carried over IP. This option utilizes cloud-based services, providing disaster recovery features such as call forwarding – a system in which calls can be redirected to another line in the event of a line failure. The service is fully managed with CTI working internally or with other leading communications companies. This solution offers quality, reliability and

business resilience. CTI's end-to-end solutions are future-proofed, scalable, and fully supported.

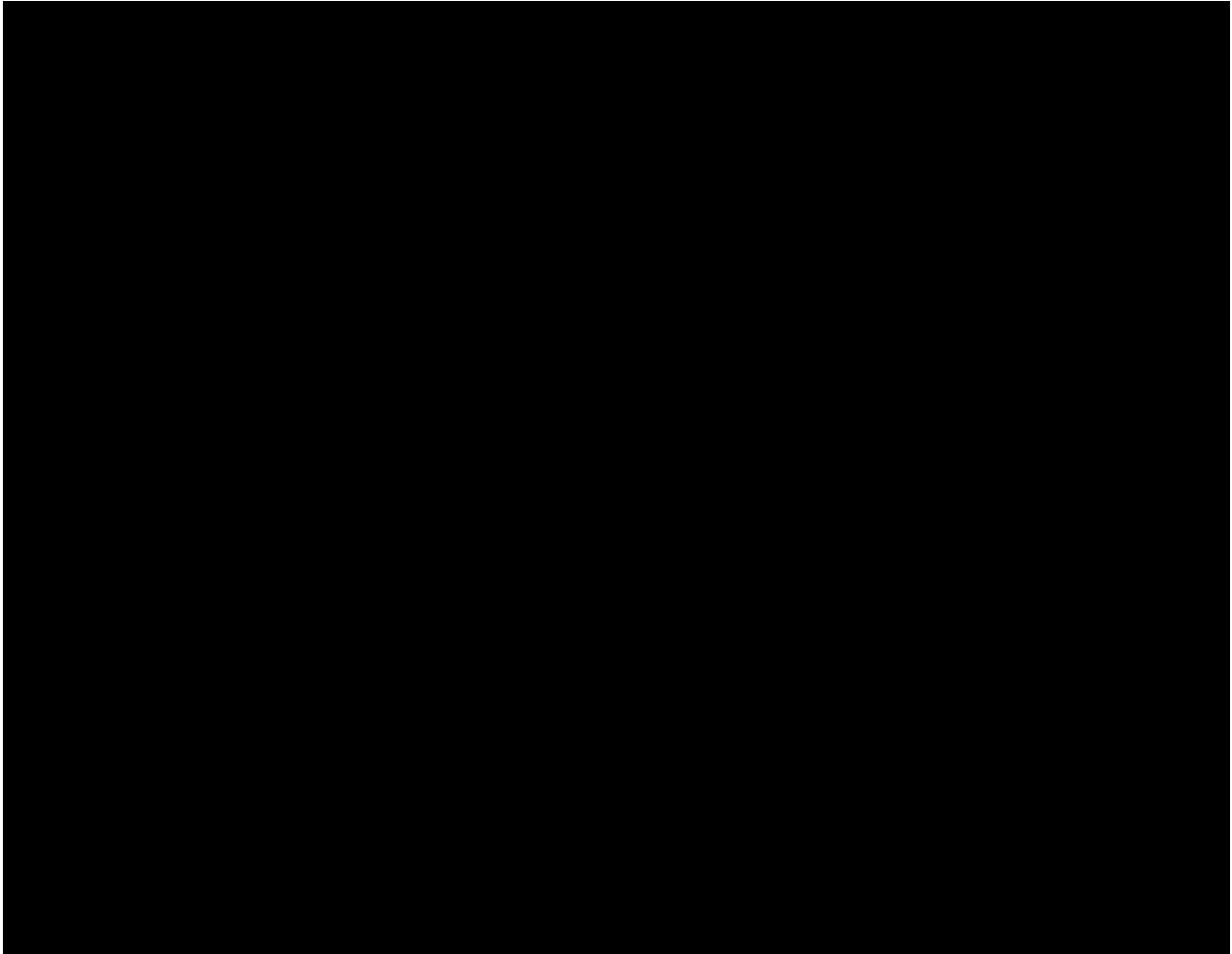


Figure 9: IPVS diagram (C.2.2.1)

2.1.1.2.1.1.1 Functional Definition (C.2.2.1.1.1) [RIN: MTR0027-DN]

[Redacted content]

[REDACTED]

[REDACTED]

[REDACTED]

CTI provides trunking to IP-PBX and PBX systems in the form of SIP, PRI, and analog trunks.

CTI can provide a hosted PBX solution with onsite customer handsets. The hosted platform can include a Unified Communications application which allows calling to and from computer desktops and mobiles devices.

CTI will provide to the customer, a premise based IP-PBX hardware system, as per requirements.

2.1.1.2.1.1.2 Standards (C.2.2.1.1.2) [RIN: MTR0020-DN]

CTI's IVPS (VoIP) trunking complies with ITU-T G.711.

CTI's IVPS (VoIP) trunking complies with SIP IETF RFC 3261 and RTP IETF RFC 3550.

H.323 is an ITU-T recommendation that defines the protocols to provide AV (Audio-Visual) communication sessions on any packet network. H-323 standards addresses call signaling and control, multimedia transport and control, and complete bandwidth control for P-T-P (Point-to-Point) or M-P (Multi-Point) conferences. CTI's network will be fully compliant and supportive of the use of H.323 within their network. H.350 is a standard, which was developed by I2MIVWG (Internet2 Middleware Initiative Video Working Group) and the ViDE (Video Development Initiative). H.350 is an LDAP (Lightweight Directory Access Protocol) object class specification that is designed to store information related to SIP, H.323, and H.320 voice and video endpoints. This stored information includes the IP addresses, aliases, and other connection related details. The CTI network offered to its customers will fully support and be compliant with the H.350 LDAP standards.

2.1.1.2.1.1.3 Connectivity (C.2.2.1.1.3)

CTI's IPVS will connect to and interoperate with:

1. PSTN, including both wireline and wireless networks, in domestic and non-domestic locations
2. All other EIS CTIs' voice service networks
3. Satellite-based voice networks

2.1.1.2.1.1.4 Technical Capabilities (C.2.2.1.1.4) [RIN: MTR0028-DN]

The IPVS will include unlimited on-net to on-net and on-net to CONUS off-net calling.

The IPVS will support off-net calling to CONUS, OCONUS, and Non-Domestic locations. CTI will provide our current commercial services that enable IPVS users to establish and receive telephone calls between both on-net locations and the PSTN.

CTI will provide a remote access capability that, once enabled, provides users with the ability to use any landline or cell phone to make or receive phone calls as if they were making or receiving calls with IPVS phones.

CTI will offer the following capabilities:

1. Real time transport of voice, facsimile, and TTY communications
2. Real time delivery of Automatic Number Identification (ANI) information (when provided from the originating party)
3. Interoperate with public network dial plans (e.g., North American Numbering Plan and ITU-E.164)
4. Interoperate with private network dial plans and support direct dialing
5. Provide access to public directory and operator assistance services
6. Provide unique directory numbers for all on-net government locations, including support for existing government numbers.
7. Provide the capability to initiate automatic callback
8. Support 3-way calling

CTI will provide gateways for interoperability between CTI's IP-based network and the PSTN, or with agency UNIs. The specific gateway will depend upon the ordering agencies UNI requirements. The gateways and functionality are described below:

1. Subscriber Gateway – CTI will provide interoperability for non-IP telephone devices. CTI will provide non-proprietary telephony station UNIs including (a) analog station and (b) ISDN BRI station interfaces.
2. PSTN Gateway – CTI will provide transparent access to and interwork with the domestic and non-domestic PSTNs.

CTI will provide the capability to support station mobility. Station mobility enables IP subscribers to dynamically move IP phones within the agency’s enterprise wide network and access IP services.

CTI’s IPVS will have the capability to traverse and successfully interoperate with agency firewalls and security layers. CTI will verify with the agency that the agency firewall is compatible with CTI’s service.

CTI will ensure that security practices and safeguards are provided to minimize susceptibility to security issues and prevent unauthorized access. This includes SIP-specific gateway security for SIP firewalls, where applicable. CTI will ensure that security practices and policies are regularly updated and audited. The general areas of security to be addressed are:

1. Denial of service – CTI will provide safeguards to prevent hackers, worms, or viruses from denying legitimate users from accessing IPVS.
2. Intrusion – CTI will provide safeguards to mitigate attempts to illegitimately use IPVS.
3. Invasion of Privacy – CTI will ensure that IPVS is private and that unauthorized third parties cannot eavesdrop or intercept IPVS communication numbers, IP addresses or URLs.

CTI will fully comply with emergency service requirements, including 911 and E911 services, and identify the location of originating stations and route them to the appropriate Public Safety Answering Point (PSAP).

CTI’s IPVS will comply with the Federal Communications Commission (FCC) Local Number Portability (LNP) requirements.

[REDACTED]

[REDACTED]

[REDACTED]

1. Real time transport of voice, fax, and TTY is supported on CTI's AS. The analog ports for fax and TTY are accomplished using a gateway such as audiocodes to accept the physical analog interface and convert it to SIP and register to CTI's AS.
2. ANI delivery is a native function of SIP messaging. CTI's AS will deliver that information across all call flows.
3. CTI's AS interoperates with public dial plans either with or without leading trunk codes such as "9"
4. CTI's AS supports short internal dialing plans while simultaneously supporting PSTN dial plans. Virtual Networks (VNET) dialing is fairly common in large enterprises.
5. CTI's AS can support agency specific 700 numbers as part of the dial plan.
6. CTI's AS can access a public or private LDAP database for directory. Customers typically use their internal Active Directory as the directory source.
7. CTI will work with our Carrier partners to provide directory numbers for each location including existing published numbers.
8. CTI's AS supports auto call back features. This can be accomplished via the voicemail platform or easily accessing calling history functions on SIP phones or clients.
9. 3-way calling is a native feature within CTI's AS. CTI's AS supports and interoperates with a wide variety of PSTN gateways to deliver the solution best suited for the customer application. There are several manufacturers that support TDM to SIP gateways for analog and ISDN BRI Interfaces. The most popular gateway is the Mediant series from Audiocodes. This same line of gateways can be used to deliver the ISDN PRI interfaces to the PSTN gateway when SIP trunks are not being used. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] The architecture is very similar in nature to what has been JITC approved for use in DoD applications.

10. CTI's AS has safeguards in place to counter DoS attacks while maintaining calls in progress. DoS protection is also a function of the network hosting the voice and video applications.

11. CTI's AS has inherent security features to protect against intrusions from either unauthorized users or administrators.

12. CTI's AS employs TLS and SRTP to encrypt both the signaling as well as the media for voice communications preventing eavesdropping or unauthorized access to audio streams. CTI's AS supports 911 and e911 requirements. It can also interoperate with 3rd Party 911/e911 applications such as Redsky or Conveyant. CTI's AS complies with FCC and as well as Carrier Features such as Local Number Portability.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.1.1.2.1.2 Features (C.2.2.1.2)

The following IPVS features will be provided:

ID Number	Name of Feature	Description
1	Voice Mail Box	CTI will offer voice mail capability that includes voice messaging transmission, reception, and storage 24x7 with the exception of periodic scheduled maintenance. CTI-provided voice mailbox will meet the following requirements:

		<ol style="list-style-type: none"> 1. Sixty minutes of storage time (or 30 messages) 2. Ability to remotely access voice mail services 3. Secure access to voice mail via a password or PIN 4. Automatic notification when a message is received 5. Message length of two minutes 6. Capability to record custom voice mail greetings <p>This capability can be administered on a station basis according to the ordering agency's needs.</p> <p>CTI will send an email with a WAVE (.wav) file attachment of each voicemail message received by users of this feature to the email address that the user designates.</p> <p>CTI will provide users the capability to add other notification devices / email addresses or to update email information and email preferences when receiving and forwarding messages through a secure user web portal.</p>
2	Auto Attendant	<p>Auto Attendant allows callers to be automatically transferred to an extension without the intervention of an operator. CTI will provide capabilities allowing callers to dial a single number for high volume call areas and to select from up to nine (9) options to be directed to various attendant positions, external phone numbers, mailboxes or to dial by name or extension.</p>
3	Augmented 911/E911 Service	<p>CTI will appropriately populate a 911 Private Switch/Automatic Location Identification (PS/ALI) database with the government's profile which will include all the users' telephone numbers, station locations, building location, building address, building floor, and room number during service implementation. CTI will provide secure remote access to the government via a client or a web browser to allow the government to maintain the government's profile on an ongoing basis (e.g., to account for moves, adds, deletions, or other changes). CTI will ensure these government profile updates are reflected in the PS/ALI database.</p>

Table 6: IPVS features table (C.2.2.1.2)

The following standard features will be included in the basic service that CTI provides:

1. Caller ID
2. Conference Calling
3. Do Not Disturb
4. Call Forward – All
5. Call Park
6. Hotline
7. Call Forward – Busy
8. Call Pickup
9. Hunt Groups

10. Call Forward – Don't Answer
11. Class of Service Restriction
12. Multi-Line Appearance
13. Call Hold
14. Distinctive Ringing
15. Directory Assistance
16. Call Transfer
17. Call Waiting
18. Speed Dial
19. Call Number Suppression
20. Specific Call Rejection
21. Last Number Dialed
22. IP Telephony Manager (Administrator)
23. IP Telephony Manager (Subscriber)

2.1.1.2.1.3 Interfaces (C.2.2.1.3)

The following UNIs at the SDP will be provided:

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	Router or LAN Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100 Mbps	SIP (IETF RFC 3261), H.323, MGCP, or SCCP

Table 7: IPVS Interfaces table

2.1.1.2.1.4 Performance Metrics (C.2.2.1.4)

The following performance levels and AQL of KPIs for IPVS will be provided:

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)
Latency	Routine	200 ms	≤ 200 ms
Grade of Service (Packet Loss)	Routine	0.4%	≤ 0.4%
Availability	Routine	99.6%	≥ 99.6%

	Critical	99.9%	≥ 99.9%
Jitter	Routine	10 ms	≤ 10 ms
Voice Quality	Routine	Mean Opinion Score (MOS) of 4.0	MOS ≥ 4.0
Time to Restore	Without Dispatch	4 hours	≤ 4 hours
	With Dispatch	8 hours	≤ 8 hours

Table 8: Performance Metrics (C.2.2.1.4)

2.1.1.2.1.5 Managed LAN Service (C.2.2.1.5)

CTI will provide a Managed LAN Service. CTI will provide and manage all LAN networking hardware components (e.g. Layer 2 switching devices, routers, switches, call servers, etc.) to extend the IPVS from the site demarcation point to the terminating user device (e.g., handset), including the management of the router that terminates the IPVS access arrangement. Equipment provided by CTI will support Power over Ethernet (PoE) in order to supply necessary power to IP phone sets or other PoE devices. IPVS service is a pre-requisite for Managed LAN Service.

CTI will provide, manage, maintain, and repair or replace all equipment necessary to provide the Managed LAN Service, except for those portions of the service for which the government is responsible (e.g., power, facilities, rack space, cabling/wiring).

CTI will provide the technical capabilities of the Managed LAN service as specified below:

1. CTI will provide all hardware and licensing necessary to extend the IPVS site demarcation point to the terminating device (e.g., the handset), for both hosted and premises-based solutions. In the case of an on-premises solution this includes any hardware or licensing necessary to support on-premises call processing (e.g., call manager, IP PBX, etc.).
2. CTI's hardware/software solution will interoperate with the ordering agency's provided IPVS-ready cabling infrastructure, including category 5, 5E, 6, 6A and single mode and multimode fiber at a minimum. CTI will identify any cabling limitations with regard to either form of IPVS solution in its proposal.

3. CTI will be responsible for the ongoing maintenance and upgrades of CTI-owned equipment used to provide the Managed LAN Service. If CTI replaces, makes any changes to CTI's equipment or device software, or reprograms user devices in order to meet the required service performance level, the government will not incur any additional cost.
4. CTI will propose installation time intervals for additional user devices at sites already using a Managed LAN Service.
5. The Managed LAN Service will not include any wireless devices or components on the LAN (i.e., wired solution only) unless requested and approved by the OCO.
6. The Managed LAN Service will not support other services (i.e., data, video, etc.) unless requested and approved by the OCO.
7. CTI will ensure that only authorized devices (as determined by the ordering agency) are able to operate on the Managed LAN Service.
8. CTI will monitor, manage, and restore the Managed LAN Service on a 24x7 basis.
9. CTI will specify the LAN management activities provided as part of the Managed LAN Service as well as identify those activities which are considered customer responsibilities in the following areas:
 4. Configuration management
 5. Moves, Adds, Changes, Disconnects (MACDs)
 6. Service/Alarm monitoring and fault management
 7. Ticket creation
 8. Proactive notification
 9. Trouble isolation and resolution
10. CTI will provide proactive notification of major and minor alarms to the Managed LAN Service via e-mail to the Points of Contact (POCs) identified by the ordering agency. Alarm notifications will be sent to all identified POCs within 15 minutes of alarm detection by CTI.

11. CTI will define the escalation path for trouble tickets for both network and hardware issues. This escalation path will be identified by level of severity and will include personnel for each level of escalation, as well as guidelines and timing for the next step in escalation.

2.1.1.2.1.6 Session Initiating Protocol Trunk Service (C.2.2.1.6)

Session Initiation Protocol (SIP) Trunk Service provides a SIP-based IP Trunk service that interoperates with any Private Branch Exchange (PBX) systems that support SIP-based IP Trunk interfaces.

SIP Trunk Service provides a direct IP connection between a SIP-enabled PBX system on an agency's premises and CTI's SIP-compliant IPVS network. SIP trunking will be fully integrated with IPVS to support calling to on-net and off-net locations. The network and its management will be provided by the underlying network service.

2.1.1.2.1.6.1 Technical Capabilities (C.2.2.1.6.1)

CTI will provide capabilities that enable SIP users to successfully establish and receive telephone calls between both on-net locations and the PSTN.

2.1.1.2.1.6.2 Features (C.2.2.1.6.2)

The following SIP Trunk Service features will be provided:

1. Automatic call routing
2. Bandwidth QoS management
3. Trunk bursting
4. Telephone number blocks (DID)

2.1.1.3 Managed Network Services (C.2.8.1)

2.1.1.3.1 Service Description (C.2.8.1.1) [RIN: MTR0129-DN]

Managed Network Service (MNS) offers a complete network management solutions designed to meet Agency requirements. With MNS, CTI provides overall management of an Agency's infrastructure, including real-time network monitoring, streamlined troubleshooting, and rapid service restoration.

When MNS is used with a single EIS service (e.g., VPNS) or a group of EIS services (e.g., VPNS, Ethernet, voice service, and cloud IaaS) requested in a TO, those services will have the functionalities of a managed service (i.e., Managed VPNS, Managed Ethernet, Managed voice service, and Managed Cloud IaaS). CTI shall use the appropriate labor and equipment as defined in GSA EIS RFP Section C.2.10. Service Related Equipment and Section C.2.11 Service Related Labor in the TO.

The basic MNS concept is illustrated below. CTI provides the design, engineering, and project management aspects, as well as other functional requirements to satisfy Agency requirements. Networks specific to a different Agencies vary in complexity in terms of size, bandwidth, and functionality. CTI acts as the Agency's single point of accountability for the networks managed under this service including operations, maintenance, and administrative activities.

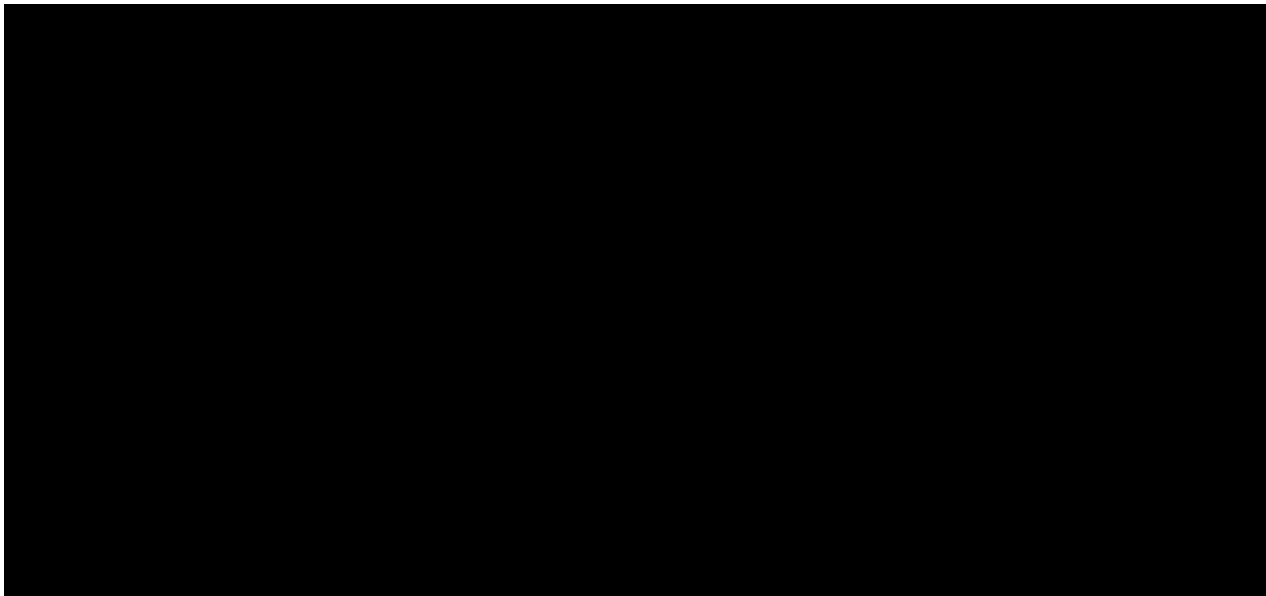


Figure 10: MNS diagram

2.1.1.3.1.1 Functional Definition (C.2.8.1.1.1)

As the World-Wide-Web expands across the globe to reach even the most remote villages, and as the Internet of Things (IoT) expands globally, especially in urban and metropolitan areas, CTI is continually expanding its capabilities to encompass more services, strategic product alliances, and global industry partnerships, simply because more and more businesses are out-tasking critical Netcentric functions. Large businesses are the most likely to out-task services, led by banking, insurance, and financial services, followed by medium-sized businesses, and government, with the GSA EIS solicitation as a key indicator of the direction the government is moving towards.

Commonly out-tasked services requested are:

- Managed VPN
- Intranet and Internet hosting
- Data storage
- Managed security
- Business continuance/disaster recovery
- Backbone network transport
- Managed business voice
- Managed contact centers

Specialized services are also filling important needs. Financial companies, for instance, are using content and mobile wireless services, while health-care companies are taking advantage of hosted applications. Typical services used by one or more industries include:

- Content services
- Mobile wireless services
- Broadband services
- IP communications
- Hosted applications

- E-commerce
- Customer support and help desk

Under the MNS offering, CTI provides overall management of an agency's network infrastructure, including real-time proactive network monitoring, troubleshooting and service restoration. CTI is the agency's single point of accountability for all networks managed under this service, including operations, maintenance, and administration activities.

2.1.1.3.1.2 Standards (C.2.8.1.1.2)

MNS shall comply with the following standards:

1. All appropriate standards for any underlying EIS access and transport services
2. The specific standards and requirements identified in the TO

Standards are incorporated into every component of service and/or delivery and products as specified or directed within the EIS GSA solicitation. Therefore, one of the first items to consider are standard(s) for network availability, reliability, and security. These are usually defined in a service-level agreement (SLA) or within the TO itself. The TO will define Quality of Service (QoS) across important parameters and identify security procedures and measurements. CTI requires that the TO cover, as much as possible, the activity of all routers, switches, paths and points of presence (POPs) if required, along with any other parameter that the customer deems important for the CTI Team to address. Especially important are QoS standards, typically covering mission-critical network availability, throughput, packet loss, latency, and jitter. Most government agencies cannot afford downtime, although the exact impact of a network outage varies greatly by agency, location or other parameter affecting Network availability.

2.1.1.3.1.3 Connectivity (C.2.8.1.1.3)

CTI will work with our underlying EIS offerings such as VPNS, PLS and other services as needed, to ensure seamless connectivity to agency networking environments. Because CTI is familiar with most vendors and their technologies and/or products, we understand how to work with each, in addition to understanding the general types of

issues that may arise when integrating services that may not be fully compatible with each other – even when the underlying standards are adhered to.

2.1.1.3.1.4 Technical Capabilities (C.2.8.1.1.4)

CTI provides the MNS capabilities outlined in the following subsections:

2.1.1.3.1.4.1 Design and Engineering Services (C.2.8.1.1.4.1) [RIN:

MTR0031-DN, MTR0110-DN, MTR0111-DN, MTR0120-DN, MTR0115-DN, MTR0116-DN, MTR0117-DN, MTR0118-DN, MTR0119-DN]

CTI shall provide and support design and engineering services as described in the Implementation, Management and Maintenance section which follows (2.8.1.1.4.2) that include, but are not limited to:

1. Identifying hardware and firmware (e.g., routers, switches, and other SRE), related software, and SRL required by the agency to deliver the EIS services.
2. Identifying network components and determine protocols, redundancy, traffic filtering, and traffic prioritization requirements. Recommending the appropriate performance levels and network capacities as required.
3. Provide complete project management for design, engineering, implementation, installation, access coordination, provisioning, equipment configuration, hardware testing, and service activation. Coordinate installation activities with the agency to minimize the impact on the current networking environment.

CTI shall identify necessary hardware and firmware needed to provide and support the enterprise traffic/services in accordance with EIS GSA Solicitation Section C.1.8.8 sub-para (3) so that transportation (participating traffic) between the agency traffic collection point(s) -- physical or virtual -- and the EINSTEIN enclave can occur. Participating traffic is defined as the external traffic identified as part of the Traffic Aggregation Service (i.e. DHS Task Order); and routed to and delivered from a DHS EINSTEIN enclave (i.e. DHS chosen secure locations). Participating agency traffic network traffic

is defined by the list of IP addresses and non-IP sources supplied by each agency and verified by DHS. Non-IP sources are converted to IP to be routed.

CTI shall ensure that there is no way for participating traffic to inadvertently or maliciously bypass DHS EINSTEIN enclaves, by integration testing in a test environment before merging change into the production environment. The exception will be for failsafe service during times the DHS EINSTEIN enclave is not working, which should be minimized as CTI shall provide redundant paths for Agency traffic to EINSTEIN enclaves to ensure no loss of traffic occurs due to a component failure. This will necessitate more than one EINSTEIN enclaves at CTI facilities. Traffic Filtering and Traffic Prioritization shall occur in the routers of the CTI supported and maintained network.

All traffic is aggregated and routed using Access Control Lists and VLAN tags. Traffic received from Participating Agencies will be identified, tagged with VLANs and forwarded to EINSTEIN enclaves. Traffic received from Non-participating will be forwarded to their final destinations. Traffic received from EINSTEIN enclaves, including traffic designated by the EINSTEIN enclave for delivery to US CERT, will be forwarded to their final destinations.

QoS features and rules can be assigned to traffic to prioritize routing. However, if the government furnished equipment in a DHS EINSTEIN enclave fails for whatever reason; CTI shall ensure redirection of traffic is failsafe, and return the participating traffic to its normal traffic path until the DHS EINSTEIN enclave is repaired.

CTI provided and supported hardware and firmware components include but are not limited to routers and switches, encryption devices, CSUs/DSUs, hubs, adapters, and modems, and the controlled EINSTEIN enclaves (s) which are used to receive traffic coming from DHS approved ISPs.

CTI shall identify network components and determine protocols, redundancy, traffic filtering and traffic prioritization requirements, recommending the appropriate performance levels and network capacities as required and also meet applicable routing requirements in the GSA EIS solicitation Section C.1.8.8., such as:

1. CTI will provide multiple tunneling standards, as required by an agency.
Examples include L2TP, GRE, IP-in-IP, MPLS, IPSec, and SSL/TLS.
2. CTI will provide various encryption levels, as required by an agency.
Examples include 3DES, RC4 and AES in accordance with the appropriate FIPS publications and modules.
3. CTI will provide authentication services as required by an agency. Examples include RADIUS, Internal LDAP, token integration, PKI, and X.509 certificates.
4. CTI will support IPv4 as both the encapsulating and encapsulated protocol.
5. CTI will support IPv6 as both the encapsulating and encapsulated protocol.
6. CTI will support QoS in the following standardized modes:
 - a. Best effort
 - b. Aggregate Customer Edge (CE) Interface level QoS (“hose” level)
 - c. Site-to-site level QoS (“pipe” level)
 - d. Intserv (RSVP) signaled
 - e. Diffserv marked
7. CTI will support QoS across a subset of the access networks as listed below:
 - a. 802.1p Prioritized Ethernet
 - b. MPLS-based access
 - c. Multilink Multiclass PPP
 - d. QoS-enabled wireless:
 - i. LTE
 - ii. Wireless 802.11.x
 - iii. Cable high-speed access (DOCSIS 1.1)
 - iv. QoS-enabled Digital Subscriber Line (DSL)
 - v. QoS-enabled Satellite Broadband Access
8. CTI will support one or more of the following application level QoS objectives:
 - a. Intserv model for selected individual flows
 - b. Diffserv model for aggregated flows

9. CTI will provide isolation of traffic and routing service that isolates the exchange of traffic and routing information to only those sites that are authenticated and authorized members of a VPN. CTI will provide Multi-Layered security architecture to ensure that attackers will not find a single point of entry but will be faced with multiple levels of security.
10. CTI will support multiple VPNs by allowing both permanent and temporary access to one or more VPNs for authenticated users across a broad range of access technologies using a variety of COTS products that meet the specific need of government customers.
11. CTI will provide secure routing services to provide full routing capability on the VPN platform with a secure policy across the VPN.
12. CTI will support the inclusion of encryption, decryption, and key management profiles as part of the security management system. Please see the section titled, "Managed Security Services" section 2.1.3.8.7 of this document.
13. CTI will support an agency in deploying its own internal security mechanisms in addition to those deployed by CTI, in order to secure specific applications or traffic at a granularity finer than a site-to-site basis.

CTI shall provide complete project management for design, engineering, implementation, installation, access coordination, provisioning, equipment configuration, hardware testing, and service activation. CTI will coordinate installation activities with the agency to minimize the impact on the current networking environment. CTI has completed multiple contracts with government Agencies and Civilian Agencies and has the proven past performance on GSA contracts and DoD contracts servicing world-wide network and satellite connectivity to know how to accomplish all these tasks proficiently. CTI has IT purchasing subject matter experts, test and validation personnel, information assurance/cyber security and government ethical hackers/vulnerability experts, network and system administrators, network architects, certified program managers, network installation specialists, network multi-media specialists, designers, technicians, system integrators, and installers on staff to ensure all of these services can be met at the unclassified and classified levels.

2.1.1.3.1.4.2 Implementation, Management and Maintenance (C.2.8.1.1.4.2)

1. CTI will develop, implement, and manage comprehensive solutions using our EIS services to meet agency-specific requirements. A complete client site survey will need to be conducted before any specific service needs are addressed. This includes locations, hardware, software, software licenses, certifications, hardware commonality, and any devices, keys, or other materials that may affect the network itself, other users, or any other QoS aspects. The solutions shall include, but are not limited to:
 - a. Access solutions that use a combination of different services (e.g., wireline and wireless access services) for specific agency locations, to meet agency performance metrics for availability and disaster recovery.
 - b. Transport solutions that distribute traffic over multiple CTI backbone networks to provide redundancy and carrier diversity, and vary the traffic allocation dynamically based on agency performance requirements.
 - c. Customer premises solutions that provide agency-specific interfaces, software, and equipment to meet agency requirements.
 - d. Security solutions as required by the agency.
2. CTI will supply and manage the hardware, firmware and related software required by the agency. Components include but are not limited to routers and switches, encryption devices, CSUs/DSUs, hubs, adapters, and modems.
3. CTI will provide tools to:
 - a) Monitor performance of agency-specific networks, including transport services, access circuits, and government edge routers.
 - b) Provide real-time visibility of transport and access services performance.
4. CTI will:
 - a) Manage the network in real-time on a 24x7 basis.
 - b) Support remote management capabilities from the operations center defined in the TO.

-
- c) Proactively monitor utilization and performance, probing in intervals of no more than fifteen minutes to ensure proper equipment/network operations.
 - d) Assess and report access and transport services performance and SLAs.
 - e) Assess and report on agency-specific network capacity and performance.
 - f) Address agency-specific network capacity and performance issues.
5. CTI will permit SNMP read-access data feeds that provide the agency with managed equipment information, as applicable.
 6. CTI will manage network configuration including but are not limited to the following activities:
 - a) Adding a protocol.
 - b) Adding, moving or removing Customer Premises Equipment (CPE).
 - c) Changing addressing, filtering, and traffic prioritization schemes.
 - d) Optimizing network routes.
 - e) Updating equipment software and/or configuration, including but not limited to firewall and VPN security devices.
 - f) Upgrading or downgrading bandwidth.
 - g) Implementing configuration changes for all agency-specific devices.
 - h) Maintaining a configuration database for all agency-specific devices.
 - i) Auditing government router configurations.
 7. CTI will provide IP Address Management as applicable. CTI will submit agency-completed American Registry for Internet Numbers (ARIN) justification requests for specified IP allocations in order to support the service offered.
 8. CTI will monitor and control access to equipment under its control, including limiting access to authorized personnel, and implementing passwords and user permissions as directed and approved by the agency.
 9. CTI will regularly perform off-site equipment configuration backups, in order to ensure the availability of recent configuration data for restoration purposes. CTI will provide the agency with secure access to backup logs as needed.
 10. CTI will perform necessary hardware and software upgrades, updates, patch deployments and bug fixes as soon as they become available. CTI will implement
-

updates in coordination and mutual agreement with the agency and test new releases to resolve any security concerns, ensure compatibility with the agency environment, minimize service disruptions, and maintain equipment functionality.

11. CTI will provide preventative and corrective maintenance on agency-specific devices.

[REDACTED]

[REDACTED] Regardless, CTI will:

- a) Monitor agency-specific network availability and quality of service (e.g., network delays, packet loss).
- b) Monitor access circuit availability and QoS.
- c) Monitor the government's edge router availability and performance.
- d) Monitor transport service availability at the government's network equipment.
- e) Monitor agency-specific network performance from government network equipment to government network equipment.
- f) Monitor transport service availability up to the government's network equipment.
- g) Monitor transport service performance from government network equipment to government network equipment.
- h) Provide, monitor and manage circuits for out-of-band government network equipment management.
- i) Open/close trouble ticket in agency's trouble ticketing system.

- j) Open/close trouble ticket in CTI's trouble ticketing system.
 - k) Troubleshoot access and transport services faults and coordinate faults resolution/repairs.
 - l) Troubleshoot government network equipment faults and coordinate resolution/repairs.
 - m) Troubleshoot agency-specific network faults.
 - n) Notify agency-specific network users of faults and maintenance via agency alerts.
 - o) Answer Network Operations Center (NOC) Help Desk phones and provide Tier-1 support to agency-specific network users.
 - p) Provide Tier-1/Tier-2/Tier-3 support to agency NOC for CTI access and transport services.
 - q) Provide Tier-1/Tier-2/Tier-3 support to agency NOC for the government's network equipment.
13. CTI will provide the agency with real or near-time access to the following:
- a) Installation schedule detailing the progress of activities such as the implementation of equipment, access and transport circuits, and ports, as applicable. This allows agencies to track the provisioning process through completion at any time. Near real-time access to the installation schedule is acceptable. The information may also be provided real-time either within a classified or unclassified web-based portal environment.
 - b) Network statistics and performance information including equipment data availability, throughput and delay statistics, CoS settings, and application-level performance information.

[Redacted content]

Service	Capability
---------	------------

Incident and Problem Management	Automatically detect and manage recurring incidents.
Knowledge Management	Brings key information to customers and CTI support personnel, right where and when the customer needs it.
Change Management	Documents and coordinates change request activity across you're the MNS — from data centers to desktops
Release Management	Combine multiple change requests into a single release and manage all related activity in support of a successful release
Service Request Management	Define a catalog of service request types that reflect what services you offer to internal or external customers
Self-Service	Context-aware self-service app that's social, mobile and formless
Asset Management	Complete lifecycle management of IT assets, from procurement to end-of-life
Service Level Management	Defines, tracks, and reports service levels
Configuration Management (CMDB)	Support ITSM processes with a single source of reference for our IT infrastructure and services
Virtual Chat	Self-service feature combines a virtual agent and live chat to improve productivity, lower IT support costs, and boost customer satisfaction
Custom Applications	Allows CTI to build everything from simple forms, to two-way integrations, to rich applications to meet customer needs.
Platform Administrations	Easily allows CTI to manager customer or organic servers, LDAP and email integrations, application and security preferences and security logs

Table 9: Services provided by Smart Reporting

d) Security logs

14. CTI will provide inventory tracking tool(s) to maintain and track all agency circuit, transport service and equipment inventory information.

15. CTI will provide the agency with secure access to current and historical information which includes, but is not limited to, the following:

- a) Bandwidth and service quality information
- b) Burst analysis identifying under or over utilization instances
- c) Data errors
- d) Delay, reliability and data delivery summaries
- e) End-to-end network views
- f) Exception analysis

- g) Link, port and device utilization
- h) Network statistics
- i) Protocol usage
- j) CPU utilization
- k) Traffic, port and protocol views

2.1.1.3.2 Features (C.2.8.1.2) [RIN: MTR0054-DN]

CTI shall provide the following features:

1. **GFP and SRE Maintenance.** CTI shall maintain and repair GFP and SRE and shall confer with government clients for a solution if any item is deemed not economically repairable.
2. **Agency-Specific Network Operations Center (NOC) and Security Operations Center (SOC).** CTI shall provide agency-specific help desk services and shared or dedicated NOCs and SOCs to meet agency requirements. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] Our Tier 1 personnel currently escalate more challenging issues to Tier 2 within two hours and to Tier 3 within three hours. We analyze all system or equipment failures and network degradations to determine the cause and establish steps required to prevent similar future issues, providing After Action Reports (AAR) up the chain of command or management chain as appropriate.
3. **Network Testing.** CTI shall support agency-specific development services which address the agency's potential need to test equipment, software and applications. This shall be accomplished on CTI's network prior to purchase and deployment. Testing shall cover voice, data, and video technologies that include but are not limited to, IP VPN and voice services. Testing shall be performed at the agency's discretion and structured in collaboration with CTI either at CTI's headquarters or with the appropriate CTI partner depending upon type and classification of

network tested. CTI will create testing environments to include sufficient equipment, software and licenses in order to replicate voice, data, video technologies and services that will be supplied to the government. Within this test environment, CTI will be able to check equipment capability, interoperability, delivery of services, and compare, prior to any delivery, any baseline changes. Baseline changes deemed to have an impact on operations, or to have an adverse effect on performance will be applied, and the unit tested on a development rack, then merged onto an integration test rack; performance tested then delivered for installation.

- 4. Traffic Aggregation Service (DHS Only).** CTI shall establish and maintain secure facilities ("DHS EINSTEIN Enclaves") where DHS-furnished equipment can be deployed, provide network connectivity from the DHS EINSTEIN Enclave to the DHS data centers, and route all traffic subject to National Policy requirements described in GSA EIS RFP Section C.1.8.8 through (i.e., deliver to and receive from) a DHS EINSTEIN Enclave for processing by the latest generation of EINSTEIN capabilities. Once traffic is received at the EINSTEIN Enclave and processed, it is sent back to CTI for delivery to its destination. Upon receipt of the EINSTEIN enclave(s), CTI will place the enclave(s) into a team member's or CTI's (when built) secure compartmented intelligence facility (SCIF) or a secure network cage and adjacent to a network testing environment as referenced above. CTI shall assume responsibility for maintaining and repairing the traffic aggregation service, including associated commercial security services and all communications links, and shall provide engineering support to integrate the DHS GFP sensor equipment, data center and communications infrastructure into the CTI's services.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.1.1.3.3 Interfaces (C2.8.1.3)

The CTI MNS will support UNIs for all underlying EIS access and transport services, as outlined in features.

2.1.1.3.4 Performance Metrics (C.2.8.1.4) [RIN: MTR0053-DN]

CTI shall meet each of the listed Key Performance Indicators (KPIs) and if applicable identify where we will exceed the stated KPIs. MNS performance levels will be specified in the TO.

2.1.1.4 Access Arrangements (C.2.9) [RIN: MTR0063-DN]

2.1.1.4.1 Access Arrangement Description (C.2.9.1)

CTI shall provide and support Access Arrangements (AAs) that connect the SDP at the agency location to a POP on our network. The range of line speeds and reliability options that CTI offers through our partners allows agency users to satisfy their diverse needs in accessing the various CTI networks. AAs provide the convention to specify and price the originating and/or terminating access component required to deliver a service. AAs cannot be ordered as a standalone access service and no performance metrics are specified for them. CTI shall meet and exceed, wherever possible, the mandatory technical capabilities written below through our teaming partners

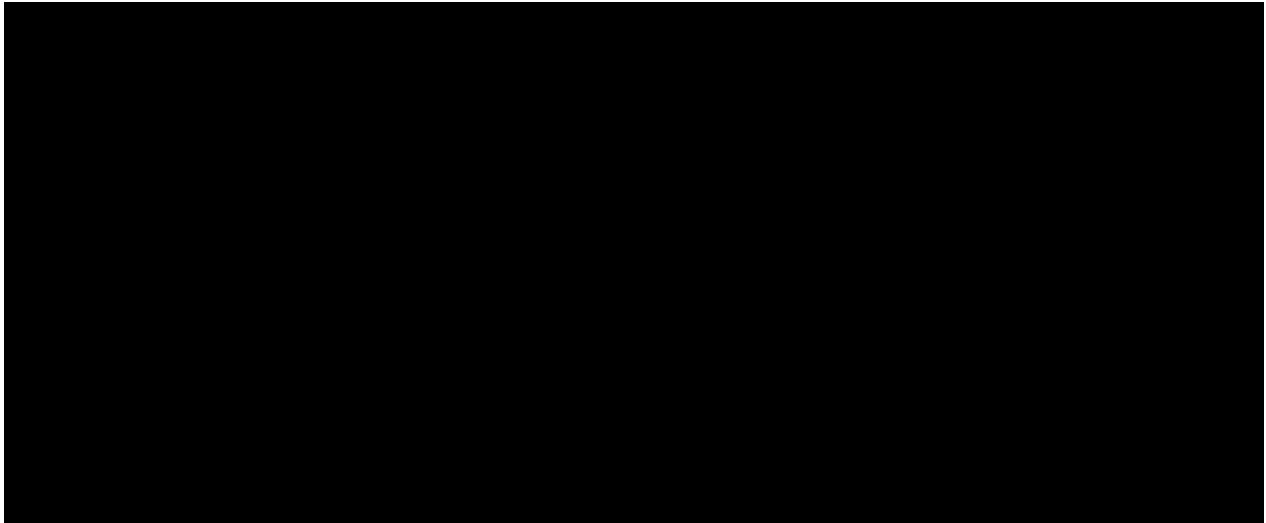


Figure 11: Access Arrangement diagram

2.1.1.4.1.1 Functional Definition (C.2.9.1.1)

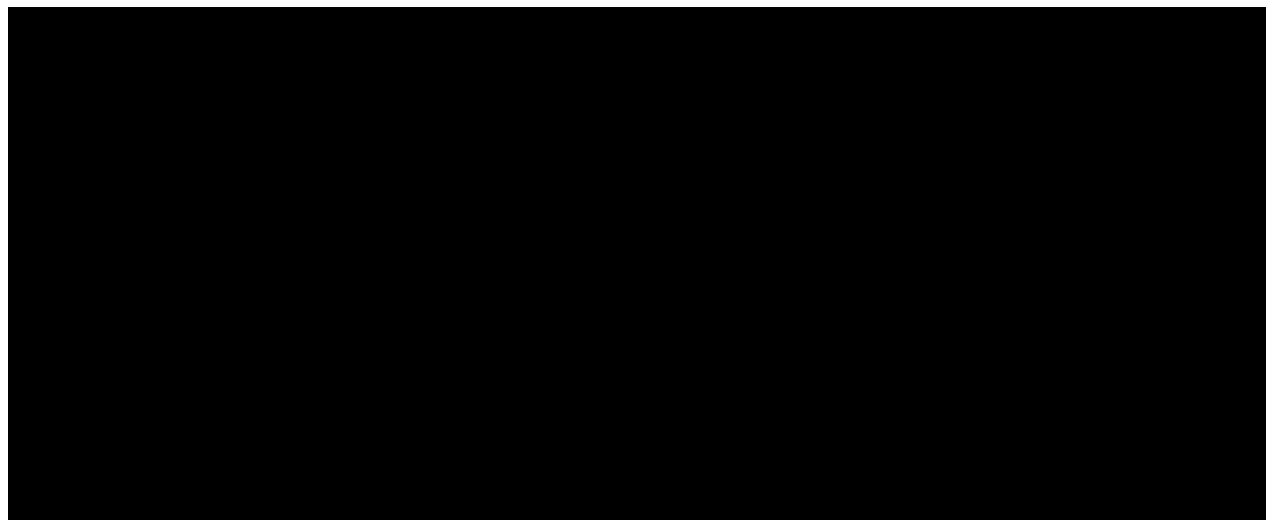


Figure 12: Access Arrangement Functional definition diagram

AAs can be used for any application such as voice, data, video, and multimedia. AAs will provide diversity options that include, but are not limited to:

1. Physically disparate, diverse paths from the SDP to the POPs of two diverse contractors.
2. Physically disparate, diverse paths from the SDP to CTI's POP.
3. Redundant paths from an SDP to CTI's POP.

In some cases access arrangements may have to be customized by CTI with special construction. Special construction may involve providing a special service or facility related to the delivery and/or performance of a service requirement by the customer.

This includes the following situations:

1. An access arrangement does not exist or does not have sufficient capacity, and CTI has to provide special construction through the implementation, rearrangement, or relocation of physical plant solely for the government-requested access arrangement.
2. The CTI Team uses special construction to implement a different route (government premises to a PCL, PCL to an alternate CTI POP, or some other type of route) than what we would otherwise use to provide an access arrangement for the government.

When necessary to fulfill an order, CTI will perform site surveys of potential operational locations to collect and validate floor plans, physical measurements, HVAC requirements, building power capacity, and external ingress/egress factors. The CTI Team will deliver site survey reports after the completion of the physical site visits. Work will not commence until CTI and the customer go over the results of the site survey to determine any impacts to cost, schedule and performance.

2.1.1.4.1.2 Standards (C.2.9.1.2)

CTI AAs comply with the following standards:

1. ANSI T1.102/107/403/503/510 for T1
2. ANSI T1.607/610 for ISDN PRI
3. Telcordia PUB GR-499-CORE for T3
4. ANSI T1.105 and 106 for SONET
5. Telcordia PUB GR-253-CORE for SONET
6. ITU-TSS G.702 and related recommendations for E1 and E3
7. Frequencies grid and physical layer parameters for Optical Wavelength:
DWDM: ITU G.692 and G.694 as mandatory and G.709 and G.872 as optional
WDM: ITUG.694.2 and Telcordia GR 253

8. Applicable Telcordia for DWDM systems are GR-1073, GR-1312, GR-2918, GR-2979 and GR-3009
9. EIA/TIA-559, Single Mode Fiber Optic System Transmission Design
10. Telcordia GR-20-CORE for Generic Requirements for Optical Fiber and Optical Fiber Cable GR-253 (SONET), and GR-326 (Connector)
11. Digital Subscriber Line (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)
12. ISDN based DSL (IDSL): ISDN Forums
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 802.3ba)
14. Cable High-Speed Service: DOCSIS (Cable Labs) standards
15. The CTI Team will comply with all new versions, amendments, and modifications to the above documents and standards.

2.1.1.4.1.3 Connectivity (C.2.9.1.3)

CTI AAs connect to and interoperate with:

1. Agency-specified locations and equipment
2. Our own network POPs

2.1.1.4.1.4 Technical Capabilities (C.2.9.1.4) [RIN: MTR2245-DN, MTR2250-DN]

CTI understands that the following AA capabilities are mandatory unless marked optional:

1. Integrated access of different services
2. Transparent to any protocol

CTI understands the following AAs are mandatory unless marked optional:

-
1. **T1.** A line rate of 1.544 Mbps, which may be used to provide channelized or unchannelized T1 access arrangement as follows:
 - a) Channelized T1. In this mode, 24 separate DS0s clear channels of 56/64 kb/s will be supported.
 - b) Unchannelized T1. In this mode, a single 1.536 Mbps information payload will be supported.
 2. **ISDN PRI.** This category of AA will support 23 separate DS0 clear channels of 56/64 kbps over an interface of ISDN PRI (23B+D) with a line rate of 1.544 Mbps.
 3. **ISDN BRI.** This category of AA will support 2 separate DS0 clear channels of 56/64 kbps over an interface of ISDN BRI (2B+D) with a line rate of 144 Kbps.
 4. **T3.** This category of AA will support a line rate of 44.736 Mbps, which may be used to provide channelized or unchannelized T3 access arrangement as follows:
 - a) Channelized T3. In this mode, 28 separate DS1 channels of 1.536 Mbps information payload rate will be supported.
 - b) Unchannelized T3. In this mode, a single 43.008 Mbps payload will be supported.
 5. **E1.** This category of AA will support a line rate of 2.048 Mbps, which may be used to provide channelized or unchannelized E1 service as follows:
 - a) Channelized E1. In this mode, 30 separate DS0 clear channels will be supported.
 - b) Unchannelized E1. In this mode, a single 1.92 Mbps information payload will be supported.
 6. **E3.** This category of AA will support a line rate of 34.368 Mbps, which may be used to provide channelized or unchannelized E3 service as follows:
 - a) Channelized E3. In this mode, 16 separate E1 channels will be supported.
 - b) Unchannelized E3. In this mode, a single 30.72 Mbps information payload will be supported.
-

-
7. **SONET OC-3.** This category of AA will support a line rate of 155.520 Mbps, which may be used to provide channelized OC-3 or concatenated OC-3c access arrangement as follows:
- a) Channelized OC-3. In this mode, three separate OC-1 channels, each with an information payload data rate of 49.536 Mbps, will be supported.
 - b) Concatenated OC-3c. In this mode, a single channel equivalent to information payload data rate of 148.608 Mbps will be supported.
8. **SONET OC-12.** This category of AA will support a line rate of 622.080 Mbps, which may be used to provide channelized OC-12 or concatenated OC-12c access arrangement as follows:
- a) Channelized OC-12. In this mode, 4 separate OC-3 channels, each with an information payload data rate of 148.608 Mbps, will be supported.
 - b) Concatenated OC-12c. In this mode, a single channel equivalent to an information payload data rate of 594.432 Mbps will be supported.
9. **SONET OC-48.** This category of AA will support a line rate of 2.488 Gbps, which may be used to provide channelized OC-48 or concatenated OC-48c service as follows:
- a) Channelized OC-48. In this mode, 4 separate OC-12 channels, each with an information payload data rate of 594.432 Mbps, will be supported.
 - b) Concatenated OC-48c. In this mode, a single channel equivalent to an information payload data rate of 2.377728 Gbps will be supported.
10. **SONET OC-192.** This category of AA will support a line rate of 10 Gbps, which may be used to provide channelized OC-192 or concatenated OC-192c service as follows:
- a) Channelized OC-192. In this mode, 4 separate OC-48 channels, each with an information payload data rate of 2.488 Gbps, will be supported.
 - b) Concatenated OC-192c. In this mode, a single channel equivalent to an information payload data rate of 9.510912 Gbps will be supported.
-

-
11. **(Optional) SONET 768.** This category of AA will support a line rate of 40 Gbps, which may be used to provide channelized OC-768 or concatenated OC-768c service as follows:
- a) Channelized OC-768. In this mode, 4 separate OC-192 channels, each with an information payload data rate of 9.510912 Gbps, will be supported.
 - b) Concatenated OC-768c. In this mode, a single channel equivalent to an information payload data rate of 38.486016 Gbps will be supported.
12. **(Optional) Analog Line (4 KHz).** This category of AA from CTI will support 2 wire analog lines and trunks without access integration for voice service.
13. **DS0.** This category of AA will support information payload data rates of 56 kbps and 64 kbps.
14. **(Optional) Subrate DS0.** This category of AA will support Sub-rate DS0 at information payload data rates of 4.8, 9.6, and 19.2 kbps.
15. **Optical Wavelength.** Bi-directional wavelengths (WDM) connections to an optical network for the following speeds:
- a) 1 Gbps
 - b) OC-48
 - c) OC-192
 - d) OC-768 (Optional)
16. **(Optional) Dark Fiber.** CTI Dark Fiber will support the following capabilities:
- a) Deployed fiber will support both single-mode and multimode fibers.
 - b) Deployed fibers will be capable of supporting a minimum of 80 DWDM wavelengths or user data with spacing as specified in ITU-T G.694.1.
 - c) Deployed fibers will be capable of operating in the "C", "D", "L" and "S" bands.
17. **Digital Subscriber Line (DSL) Access Arrangements:**
- a) CTI will provide the following types of DSL services, at a minimum:
 - 3. Asymmetric DSL (ADSL). Support ADSL asymmetric data rates for upstream and downstream traffic as follows:

16. Upstream: Data rates will range from 16 to 768 kbps (e.g., 256 kbps).

17. Downstream: Data rates will range from 1.5 Mbps to 8 Mbps (e.g., at 1.5, 2, 3, 4, 5, 6, 7, and 8 Mbps). Speeds up to 9 Mbps are optional.

4. Symmetric DSL (SDSL). Support SDSL symmetric (i.e., same) data rates for both upstream and downstream traffic at data rates up to and including 1.5 Mbps. 2.3 Mbps is optional.
5. (Optional) ISDN DSL (IDSL). Support ISDN symmetric (i.e., same) data rates for both upstream and downstream traffic at data rates of 144 Kbps.

18. Ethernet Access Arrangements:

a) CTI shall provide and support Ethernet Access Arrangements will support both dedicated access and/or shared access (multiplexed Ethernet connections) over a Metro Ethernet service from SDP to POP. CTI will support access speeds of:

1. 1 Mbps to 10 Mbps at 1 Mbps increments
2. 10 Mbps to 100 Mbps at 10 Mbps increments
3. 100 Mbps to 1000 Mbps at 100 Mbps increments
4. 1 Gbps to 10 Gbps at 1 Gbps increments
5. (Optional) 10 Gbps to 100 Gbps at 10 Gbps increments

For each of the access connections, CTI will maintain appropriate committed bandwidth or CIR (Committed Information Rate), as supported by the MEF 33 - Ethernet Access Services standard and the MEF Bandwidth Profiles for Ethernet Services and as specified in the TO.

19. (Optional) Cable High-Speed Service Access Arrangements:

a) Provide data rates of 256 Kbps to 30 Mbps as follows:

6. From 256 Kbps to a maximum of 5 Mbps (Standard: DOCSIS 1.0)
7. From 256 kbps to a maximum of 10 Mbps (Standard: DOCSIS 1.1)
8. From 256 kbps to a maximum of 30 Mbps (Standard: DOCSIS 2.0)

20. (Optional) Fiber-To-The-Premises (FTTP):

- a) 5 Mbps (downstream) and 2 Mbps (upstream)
- b) 15 Mbps (downstream) and 2 Mbps (upstream)
- c) 30 Mbps (downstream) and 5 Mbps (upstream) and to a maximum of 150 Mbps (Standard: DOCSIS 3.0)

21. Wireless Access Arrangements:

- a) Cellular Service - 4G Long Term Evolution (LTE):
 - i. 100 mbps (downstream) and 50 mbps (upstream)
- b) Line of sight connection, using licensed frequencies:
 - i. DS1
 - ii. NxDS1 (where N=2 through 27)
 - iii. DS3
 - iv. E1 (Non-domestic)
 - v. Nx E1 (where N=2 through 15) (Non-domestic)
 - vi. E3 (Non-domestic)
 - vii. SONET OC-3
 - viii. 1 Gbps, 5 Gbps and 10 Gbps

2.1.1.4.2 Access Diversity and Avoidance (C.2.9.2)

The following are mandatory unless marked optional:

ID Number	Name of Access Capability	Description
1	Access Route or Path Diversity	CTI will supply at least two physically-separated routes for access diversity with the following options: <ol style="list-style-type: none"> 1. Between an SDP and its associated connecting network’s PCL or POP, or 2. Between an SDP and at least two connecting network PCL/POPs. 3. Access from the same or different access providers (e.g., ILEC and a CLEC) for two separate routes, using any mix of access arrangements. These diverse routes will : <ol style="list-style-type: none"> 1. Not share any common telecommunications facilities or offices including a common building entrance. 2. Maintain a minimum separation of 30 feet throughout all diverse routes between premises/buildings where an SDP and its associated network connecting point are housed. 3. Maintain a minimum vertical separation of two feet, with cables encased (separately) in steel or concrete for cable crossovers. CTI will provide the capability for the automatic switching of transmission in real-time, negotiated on an individual case basis:

		<ol style="list-style-type: none"> From the primary access route to the one or more diverse access routes, including satellite connection, and From the diverse access route to the primary access route. <p>CTI will exercise the following control measures on the configuration or the reconfiguration of the diverse access route:</p> <ol style="list-style-type: none"> CTI will provide a graphical representation (e.g., diagrams, maps) of access circuit routes to show where diversity has been implemented to the OCO within 30 calendar days of the implementation of access diversity and again thereafter when a change is made. Prior to any proposed reconfiguration of routes previously configured for access diversity, CTI will provide to the agency written notification and revised PCLs for OCO approval in accordance with the requirements of the TO. CTI will establish internal controls to prevent the dismantling of diversified routes.
2	Access Route or Path Avoidance	<p>CTI will supply the capability for a customer to define a geographic location or route to avoid between an SDP and its associated connecting network point. CTI will exercise the following control measures on the configuration or reconfiguration of the avoidance access route:</p> <ol style="list-style-type: none"> CTI will provide a graphical representation (e.g., diagrams, maps) of access circuit routes to show where avoidance has been implemented to the OCO within 30 calendar days of the implementation of avoidance and again thereafter when a change is made. Prior to any proposed reconfiguration of routes previously configured for avoidance, CTI will provide to the agency written notification and revised PCLs for OCO approval in accordance with the requirements of the TO. CTI will establish internal controls to prevent the dismantling of avoided routes.

Table 10: Access diversity and avoidance table (C.2.9.2)

2.1.1.4.3 Interfaces (C.2.9.3) [RIN: MTR0157-DN]

CTI will comply with all documented standards as per the UNI interfaces listed herein in Table C.2.9.3.

CTI understands that the UNIs at the SDP for AA are mandatory unless marked optional:

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling 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	<ol style="list-style-type: none"> Transparent IP (v4/v6)
6	ISDN PRI (23B+D and 24B+0D) [Std: ANSI T1.607/610]	Up to 1.472 Mbps	Transparent
7	T3 (Std: Telcordia GR-400-CORE)	Up to 43.008 Mbps	Transparent
8	E1 (Std: ITU-TSS)	Up to 1.92 Mbps G.702) (Non-domestic)	Transparent
9	E3 (Std: ITU-TSS G.702) [Non-domestic]	Up to 30.72 Mbps	Transparent

10	SONET OC-3 (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
11	SONET OC-3c (Std: ANSI T1.105 and 106)	148.608 Mbps	Transparent
12	SONET OC-12 (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
13	SONET OC-12c (Std: ANSI T1.105 and 106)	594.432 Mbps	Transparent
14	SONET OC-48 (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent
15	SONET OC-48c (Std: ANSI T1.105 and 106)	2.377728 Gbps	Transparent
16	SONET OC-192 (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent
17	SONET OC-192c (Std: ANSI T1.105 and 106)	9.510912 Gbps	Transparent
18	SONET OC-768 (Std: ANSI T1.105 and 106)	38.486016 Gbps	Transparent
19	SONET OC-768c (Std: ANSI T1.105 and 106)	38.486016 Gbps	Transparent
20	10 Base-T/TX/FX (Std: IEEE 802.3)	Link bandwidth: Up to 10 Mbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
21	100 Base-TX/FX (Std: IEEE 802.3)	Link bandwidth: Up to 100 Mbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
22	1000 Base-T/L/LX/B/BX/PX (Std: IEEE 802.3)	Link bandwidth: Up to 1 Gbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
23	10 Gbps (Std: IEEE 802.3)	Link bandwidth: Up to 10 Gbps	1. IP (v4/v6) 2. IEEE 802.3 Ethernet MAC (for bridging)
24	Reserved		
25	ISDN BRI (2B+D) (Multirate) [Std: ANSI T1.607 and 610]	144 kbps	1. ITU-TSS Q.931 2. IP (v4/v6)
26	3G / 4G / 4G LTE (Cellular Service)	Up to current standard	1. ITU 3GPP TR25.913 2. IP (v4/v6)

Table 11: AA Interfaces diagram (C.2.9.3)

2.1.2 EIS Scope for Optional Services (C.1.2) [RIN: MTR0161-DN]

2.1.2.1 Data Service (C.2.1)

2.1.2.1.1 Virtual Private Network Service* (C.2.1.1)

[*Mandatory Service, answered above in Section 2.1.1.1]

2.1.2.1.2 Ethernet Transport Service* (C.2.1.2)

[*Mandatory Service, answered above in Section 2.1.1.2]

2.1.2.1.3 Optical Wavelength Service (C.2.1.3)

No bid.

2.1.2.1.4 Private Line Service (PLS) (C.2.1.4)

No bid.

2.1.2.1.5 Synchronus Optical Network Services (SONET) (C.2.1.5)

No bid.

2.1.2.1.6 Dark Fiber Services (DFS) (C.2.1.6)

No bid.

2.1.2.1.7 Internet Protocol Service (C.2.1.7)

No bid.

2.1.2.2 Voice Service (C.2.2)

2.1.2.2.1 Internet Protocol Voice Service* (C.2.2.1)

**Mandatory Service, answered above in Section 2.1.1.2.1*

2.1.2.2.2 Circuit Switched Voice Service (C.2.2.2)

CTI has been providing CSVS solutions since 1999 with over 200,000 business customers with feature rich functionality to provide standard PSTN connectivity through solutions such as POTS and PRI. CTI notes that the government has a large community of circuit-switched voice users throughout the US public sector and conducts a considerable amount of business with US citizens, private sector firms, and foreign entities using circuit-switched voice. CTI will be able to address all clients and organizations the government currently works with.

2.1.2.2.2.1 Service Description (C.2.2.2.1)

CTI will provide the government with the interfaces, access, connectivity, capabilities, and all features required. Most voice calls will be provided through our circuit-switched network for both on-net and off-net communications. The foundation of service

continuity and quality is a reliable, resilient network and CTI will provide all VS that the government requires.

2.1.2.2.2.1.1 Functional Definition (C.2.2.2.1.1) [RIN: MGC0001-DI, MTR2251-DN]

CTI has all of the voice products required for the GSA EIS, including local and long distance. [REDACTED]

[REDACTED]

- | [REDACTED]
- | [REDACTED]

[REDACTED]

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

[REDACTED]

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

[REDACTED]

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

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

2.1.2.2.2.1.2 Standards (C.2.2.2.1.2)

[REDACTED]

[REDACTED]

[REDACTED]

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

2.1.2.2.2.1.3 Connectivity (C.2.2.2.1.3)

CTI's CSVS connects to and interoperates with:

1. Government-specified terminations (such as single-line telephones, Secure Terminal Equipment, multi-line key telephone systems, conference-room audio equipment, PBX, Centrex, T1 MUX, modem, FAX, and video teleconferencing systems).
2. PSTN, including both wireline and wireless networks, in domestic and non-domestic locations.
3. The voice service networks of all other EIS contractors.

4. Satellite phones and terminals.

2.1.2.2.2.1.4 Technical Capabilities (C.2.2.2.1.4)

CTI's VS supports the full range of technical capabilities that are available in commercial offerings. These capabilities include:

1. Numbering Plan:
 - a. Unique directory number for all on-net Government locations, including support for existing government numbers.
 - b. PSTN (including both wireline and wireless networks) numbers and any future changes to PSTN numbers
 - c. Non-commercial Agency specific private 700 numbers
 - i. CTI will support originating and terminating on-net calls. Incoming off-net calls from the PSTN are blocked unless an Agency specific request for the service gateway has been received and implemented.
 - d. CTI will allow transparency and interconnectivity between CTI's network and other networks. See Section 2.1.2.2.2.1.3 for more on CSVS Connectivity.
2. CTI will provide a network intercept to a recorded announcement is provided as an inherent network capability when a call cannot be completed, At a minimum, CTI will provide such announcements for the following conditions:
 - a. Number disconnected (disconnected numbers are not reassigned for at least 90 days for those situations where CTI controls number assignment).
 - b. Time-out during dialing.
 - c. Network congestion.
 - d. Denial of access to off-net and non-US calls.
 - e. Denial of access to features.
3. Voice quality at least equal to 64 kbps PCM (standard: ITU G.711)

4. CTI complies with the emergency service requirements, which includes 911 and E911 services, and will identify the locations of the originating stations and route them to the appropriate Public Safety Answering Point (PSAP).

2.1.2.2.2 Features (C.2.2.2.2)

CTI assumes the following CSVS features are mandatory unless marked optional. CTI complies with the feature requirements as stated below.

ID Number	Name of Feature	Description
1	Agency-Recorded Message Announcements	<ol style="list-style-type: none"> 1. Authorized government personnel will be able to record message announcements within the network after authentication of user-ID and password/token. 2. The recording will be assigned an on-net number and will be accessible from on-net and off-net stations. 3. CTI will provide the capability of a three-minute message announcement length. 4. The length of each message provided by the government will be determined on a case-by-case basis and will continue to three minutes in length (or longer if CTI's capability exists and is provided at no additional cost to the government). 5. A call to the announcement must be answered within five rings and barge-in access to the announcement will be permitted. 6. CTI will provide a system-wide capability for storing a minimum of 500 recorded messages. <p>This feature will enable a minimum of 250 callers concurrently to access an announcement.</p>
2 (optional)	Authorization Codes/ Calling Cards	<p>CTI will provide authorization codes that support the following functions:</p> <ol style="list-style-type: none"> 1. Caller identification and class-of-service (CoS) for users to include call screening (see User's Call Screening feature) and service performance levels (see Performance Metrics for routine and critical users). At a minimum, 128 classes of service will be available to each user, station, or trunk. 2. Same authorization code for originating on-net, off-net, and audio conference calls. 3. Use authorization code if originating station identification cannot be made by other means for billing and CoS purposes. 4. Use authorization code when override capabilities are desired. 5. The CoS derived from an authorization code will take precedence over that derived from any other means. 6. When an authorization code is used for the service, it will be verified without involving an operator before a call is connected. 7. CTI will support the following capabilities as specified by the government:

ID Number	Name of Feature	Description
		<ul style="list-style-type: none"> a. Actual requirements for calling party identification (e.g., ANI suppression). b. CoS assignment. c. Types of calling cards: <ul style="list-style-type: none"> 1. Post-paid calling cards. <ul style="list-style-type: none"> (a) Charges accumulate as the card is used, and billing is based upon monthly charges. 2. Pre-paid calling cards. <ul style="list-style-type: none"> (a) Fixed dollar amount of \$50.00 (b) Rechargeable dollar amount where amount can be renewed or increased when the initial amount balance is low or depleted d. Expiration date for pre-paid calling cards. e. Use for audio conferencing service (ACS) only. f. Agency-specific logo and no printing of GSA logo on the card. g. Suppression of call detail records (CDRs). h. Immediate cancellation of the card if reported stolen or lost by a user without incurring further charges on the card. <p>The format of the authorization code will be determined by CTI and will support/provide the following capabilities:</p> <ul style="list-style-type: none"> 1. Credit card-sized authorization code card(s), also called Calling Cards, unless otherwise directed by the government. 2. Durable plastic composition and imprinted with authorization code, user's name, and organization. 3. User instructions will be issued, as directed by the government, at no additional cost. 4. Safeguards as follows: <ul style="list-style-type: none"> a. Potential fraud and theft regarding issuance, distribution, and activation of authorization codes. b. Delivery of Personal Identification Numbers (PINs) independent from delivery of the calling cards. c. Exclusion of the last 4 digits of authorization codes (i.e., PINs) in billing records. 5. If sufficient space is available, inclusion of the Federal Relay Service's "TDD/800-877-8339" number on the back of the calling card. 6. Contractor-defined dialing sequence that alerts the network when an authorization code is about to be entered so that processing of calls not requiring this feature are not delayed. 7. Temporary override of a CoS restriction assigned to a caller's station. This will allow an individual user to place a call at a higher network CoS for the duration of the call by entering a valid authorization code. This capability will have the following functionalities.

ID Number	Name of Feature	Description
		<ul style="list-style-type: none"> a. Absence of excessive delays caused by waiting for all digits to be dialed before recognizing the call as one that involves an override. b. Inclusion of all CDR relevant data charged to the authorization code rather than to the originating station. <p>8. Allowance of authorized users to gain access, after validation of authorization codes, to on-net voice service and features from off-net locations by dialing certain contractor-provided toll free and message unit-free (to the callers) commercial directory numbers. This capability will have following functions.</p> <ul style="list-style-type: none"> a. Numbers may be a local number, a Foreign Exchange number, an NANP number, or some other service type, e.g., toll free service, for which toll free and message unit-free service has been arranged for pre-designated regions. b. Toll free and message unit-free commercial directory numbers will be printed on the back of the calling card. c. Region boundaries will be defined by CTI. d. Users will be able to select, by service order, the regions of the country from which access is to be allowed and the service type that provides the most economical service for a given application. <p>9. A multiple call feature that will allow the user to dial a code (e.g., the “pound” key [#]) after a call in order to make multiple calls without re-dialing the access and card number.</p> <p>10. Direct operator access to provide assistance with dialing or for providing information.</p> <p>11. An error correction feature that enables cardholders to correct a dialing mistake by pressing a key, e.g., the “star” key (*) and re-enter the correct number.</p> <p>12. Speed dialing that allows cardholders to use abbreviated dial codes for frequently dialed numbers.</p> <p>13. Availability of all administrative tools or management reports made available by CTI with equivalent commercial calling card offerings.</p>
3	Caller Identification (ID)	CTI will provide the calling number to the terminating stations for each incoming call.
4	Call Screening for users	<p>Call screening consists of a set of features that determine a call's eligibility to be completed as dialed based upon CoS information associated with the user, the station, or the trunk group. The following call screening features will be supported:</p> <ul style="list-style-type: none"> 1. Class of Service (CoS) and Restrictions. CTI will provide a minimum of 128 classes of service for each user, station, or trunk. <p>CoS will be determined from the ANI, authorization code, traveling classmark, or trunk group. The CoS derived from an authorization code will take precedence over that derived from other means. Classes of service will identify but not be limited to access and feature restrictions as follows:</p>

ID Number	Name of Feature	Description
4.2. (optional)		<ol style="list-style-type: none"> a. Access restrictions will include but not be limited to access to toll free and 900 calls, access to off-net calling, access to other government networks, access to non-US calling, and access to other than specified NPA/NXXs. b. Feature restrictions will allow or restrict access to network features by users or groups of users. <ol style="list-style-type: none"> 2. Code Block. This feature will screen and prevent ineligible users, stations, and trunks with certain CoS access restrictions from calling specified area codes, exchange codes, and countries. Blocked calls will be intercepted to appropriate network recorded announcements.
5 (optional)	Customized Network Announcement Intercept Scripts	CTI will implement customized network intercept announcement scripts as requested by the government. CTI will record the customized network announcements after obtaining government approval of scripts.
6 (optional)	Internal Agency Accounting Code	<p>For calls involving a calling card or originating station with a special CoS, the following capabilities will be provided:</p> <ol style="list-style-type: none"> 1. Entry of additional (up to a maximum of eight) digits to identify internal agency accounting codes for the call, i.e., these accounting codes will be transferred to the CDR with no further processing. 2. CDRs will reflect all relevant data on the call to include internal agency accounting code digits. <p>Calls will be charged to the authorization code rather than to the originating station.</p>
7	Directory Assistance	A user will be able to call off-net directory assistance by dialing NPA-555-1212 or any other off-net directory assistance number. NPA also includes service access codes (e.g., 800) for this feature.
8	Suppression of Calling Number Delivery	Based on the CoS of the originating station or calling card, CTI will inhibit the delivery of the calling number, i.e., ANI, by setting the Privacy Indicator at the originating end and honoring it at the terminating end. In addition, it will be possible to block calling number delivery on a call by call basis by dialing a contractor-provided code.
9	Voice Mail Box	<p>CTI will offer voice mail capability that includes voice messaging transmission, reception, and storage for 24x7 except for periodic scheduled maintenance. CTI provided voice mailbox will meet the following minimum requirements:</p> <ol style="list-style-type: none"> 1. At least sixty minutes of storage time (or 30 messages) 2. Ability to remotely access voice mail services 3. Secure access to voice mail via a password or PIN 4. Automatic notification when a message is received 5. Minimum message length of two minutes 6. Capability to record custom voice mail greetings <p>This capability can be administered on a station basis according to the ordering agency's needs.</p>
10 (optional)	Basic Subscriber Line: Multi Appearance Directory Number	A Multiple Appearance Directory Number is a telephone number that appears on two or more telephones.

ID Number	Name of Feature	Description
11 (optional)	ISDN PRI: Backup of Shared-D Channel	Backup of a single D channel that is controlling multiple PRIs.
12 (optional)	ISDN BRI: Multi Appearance Directory Number	A Multiple Appearance Directory Number is a telephone number that appears on two or more ISDN telephones.
13 (optional)	MLPP	DOD requires the CSVS to have Multilevel Precedence and Preemption (MLPP) capability as defined in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C and DOD Instruction 8100.3, Department of Defense Voice Networks, to specified users and on trunks connecting to the Defense Switched Network (DSN).

Table 12: Features (C.2.2.2.2)

2.1.2.2.2.3 Interfaces (C.2.2.2.3)

CTI supports the following interfaces for CSVS. CTI understands that the following UNIs at the SDP are mandatory unless marked optional.

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
1	Analog Line: Two-Wire (Basic Subscriber Line) (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Line-Loop Signaling
2	Analog Line: Four-Wire (Basic Subscriber Line) (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Line-Loop Signaling
3	Analog Trunk: Two-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk-Loop Signaling (loop and ground start)
4	Analog Trunk: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk-Wink Start Signaling
5	Analog Trunk: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Trunk-E&M Signaling
6	Digital Trunk: T1 (Std: Telcordia SR-TSV-002275 and ANSI T1.102/107/403)	Up to 1.536 Mbps	T1 Robbed-Bit Signaling
7	Digital Trunk: ISDN PRI (23B+D and 24B+0D)T Reference Point (Std: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type
8	Digital: T3 Channelized (Std: Telcordia GR-499-CORE)	Up to 43.008 Mbps	SS7, T1 Robbed-Bit Signaling
9 (Non-US)	Digital Trunk: E1 Channelized (Std: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling
10 (Optional)	Optical: SONET OC-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	SS7
11 (Optional)	Electrical: SONET STS-1 (Std: ANSI T1.105 and 106)	49.536 Mbps	SS7
12 (Non-US)	Digital: E3 Channelized (Std: ITU-TSS G.702)	Up to 30.72 Mbps	SS7, E1 Signaling
13	Digital Line: ISDN BRI (2B+D) S and T Reference Point (Std: ANSI T1.607 and 610)	Up to 128 kbps (2x64 kbps)	ITU-TSS Q.931
14	Router or LAN Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100 Mbps	SIP (IETF RFC 3261), H.323, MGCP, or SCCP

Table 13: Interfaces (C.2.2.2.3)

2.1.2.2.2.4 Performance Metrics (C.2.2.2.4)

CTI will be able to provide the following performance metrics:

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
Availability (POP-to-POP)	Routine	99.95%	≥ 99.95%	See Note 1
Availability (SDP-to-SDP)	Routine	99.5%	≥ 99.5%	
	Critical	99.95%	≥ 99.95%	
Time to Restore	With Dispatch	8 hours	≤ 8 hours	See Note 2
	Without Dispatch	4 hours	≤ 4 hours	
Grade of Service (Call Blockage)	Routine	0.07 (SDP-to-SDP)	≤ 0.07	See Note 3
		0.01 (POP-to-POP)	≤ 0.01	
	Critical	0.01 (SDP-to-SDP & POP-to-POP)	≤ 0.01	

Table 14: Performance Metrics (C.2.2.2.4)

Notes:

1. CSVS availability is calculated as a percentage of the total reporting interval time that the voice service is operationally available to the agency. Availability is computed by the standard formula:

$$Availability = \frac{RI(HR) - COI(HR)}{RI(HR)} \times 100$$

[Note that this KPI is waived for calls made with calling card.]

2. Refer to Section G.8.2 for definition and how to measure.
3. Grade of Service (Call Blockage) is the proportion of calls that cannot be completed during the busy hour because of limits in the call handling capacity of one or more network elements. For example, 0.01 indicates that 1 percent of the calls are not being completed (1 out of 100 calls).

2.1.2.2.3 Toll Free (C.2.2.3)

No bid.

2.1.2.2.4 Circuit Switched Data Service (CSDS) (C.2.2.2)

No bid.

2.1.2.3 Contact Center Services (C.2.3)

No bid.

2.1.2.4 Collocated Hosting Center Services (C.2.4)

No bid.

2.1.2.5 Cloud Services (C.2.5) [RIN: MTR0084-DN]

CTI, in accordance with NIST SP 800-145, understands the three cloud services definitions for Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). [REDACTED]

[REDACTED]

[REDACTED]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

- | [Redacted]
- | [Redacted]
- | [Redacted]
- | [Redacted]

[Redacted]

[Redacted text block]

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]

[Redacted text block]

[Redacted content]

<p>RESERVATION MODEL: DEDICATED, RESERVED RESOURCES.</p>	<p>UNDER THE RESERVATION MODEL, A DEDICATED, RESOURCE POOL OF COMPUTE, NETWORK AND STORAGE RESOURCES WILL BE RESERVED FOR A CUSTOMER WITHIN A PRIVATE VIRTUAL DATA CENTER (VDC). THE AMOUNT OF RESOURCES ASSIGNED IS BASED ON THE CUSTOMER CONTRACTED AMOUNT. THESE RESOURCES ARE DEDICATED AND ARE CONSIDERED RESERVED FOR THAT CUSTOMER. THE VDC WITH THE RESERVED RESOURCES IS MADE AVAILABLE TO THE CUSTOMER TO CONFIGURE AND PROVISION THEIR ENVIRONMENT BASED ON THEIR BUSINESS NEEDS. ALLOCATED RESOURCES TO THE CUSTOMER FROM CTI/QTS ARE NOT OVERSUBSCRIBED OR THIN-PROVISIONED. HOWEVER, CUSTOMERS HAVE THE OPTION TO OVERSUBSCRIBE THEIR VDC IF THEY SO DESIRE. CUSTOMERS WILL ALSO BE GIVEN ACCESS TO A SECOND VDC THAT OPERATES UNDER A PAY-AS-YOU-GO MODEL. THIS PROVIDES THE ABILITY TO ACCESS ADDITIONAL RESOURCES, ABOVE THE ORIGINAL COMMITMENT, ON AN AS AVAILABLE BASIS.</p>
<p>STAND-ALONE, PAY-AS-YOU-GO MODEL: PAY-PER-USE OPTION.</p>	<p>THE STAND-ALONE, PAY-AS-YOU-GO MODEL IS AVAILABLE TO CTI/QTS TEAM CUSTOMERS. UNDER THIS MODEL THERE IS NO MINIMUM FEE AND THE CUSTOMER WILL ONLY PAY FOR THE RESOURCES USED. THIS MODEL DOES NOT GUARANTEE AVAILABLE RESOURCES; RATHER THIS MODEL IS BASED ON AVAILABILITY. CUSTOMERS ARE BILLED ON AN HOURLY USAGE BASIS FOR COMPUTE AND STORAGE PLUS INTERNET UTILIZATION</p>

BASED ON MONTHLY 95TH PERCENTILE. ADDITIONAL NETWORK RESOURCES WILL BE
BILLABLE ON A MONTHLY BASIS BASED ON SIGNED WORK ORDER.

Table 15: IaaS Reservation vs Stand-alone Model

[Redacted Table Content]

[Redacted Table Content]

[Redacted Table Content]

[Redacted Table Content]

[REDACTED]

[REDACTED]

[REDACTED]

2.1.2.5.1 Infrastructure as a Service (C.2.5.1) [RIN: MTR0142-DN, MTR0160-DN, MTR0084-DN]

[REDACTED]

[REDACTED]

2.1.2.5.1.1 Service Description (C.2.5.1.1) [RIN: MTR0084-DN]

[REDACTED]

- [REDACTED]

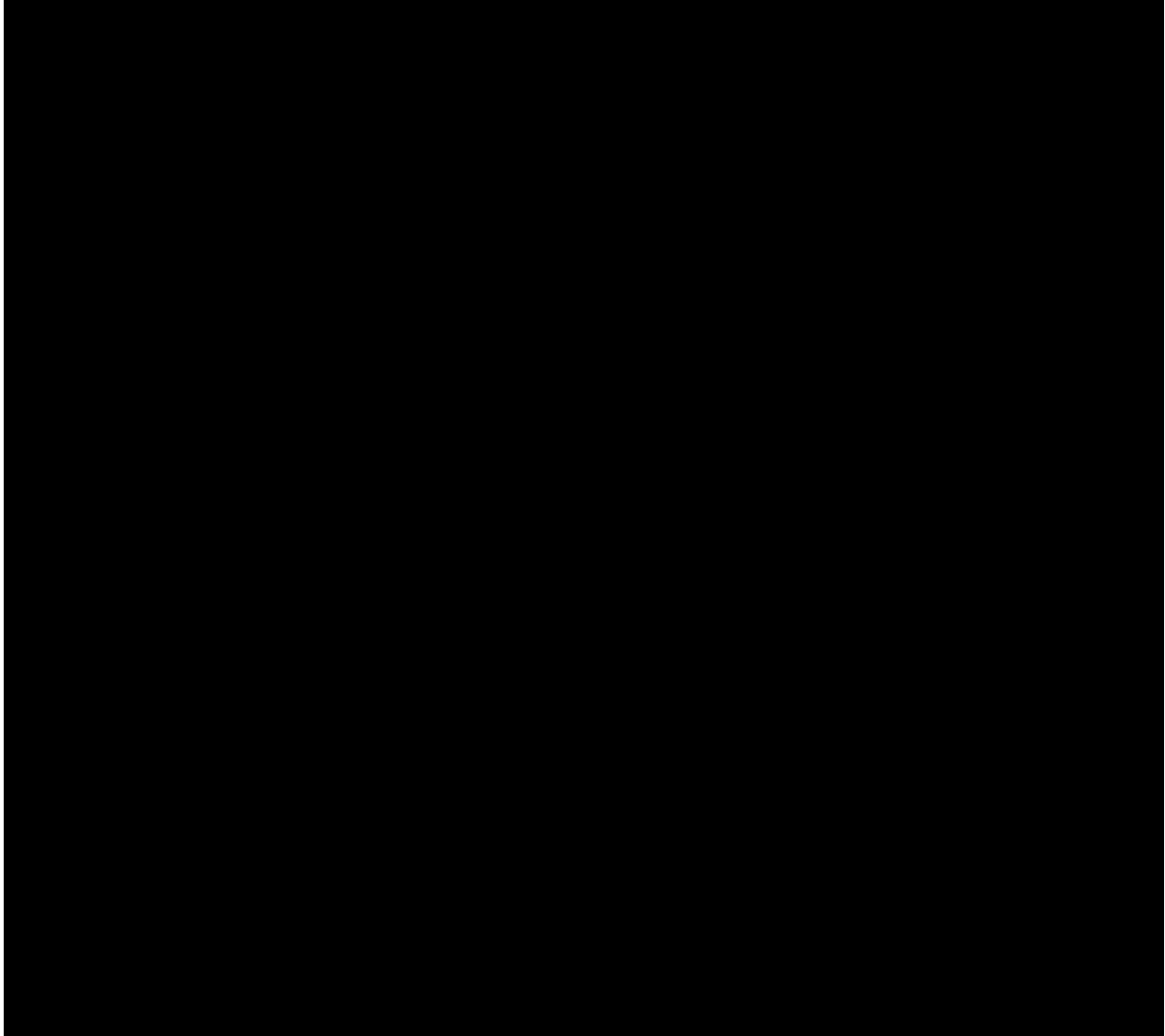
- [REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

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



[Redacted content]

[REDACTED]

[REDACTED]

[REDACTED]

CTI/QTS understands and complies with the NS/EP, Federal recovery prioritization including having Local Emergency Response Action Plans for every individual data center and environments within each data center [REDACTED]

[REDACTED]

[REDACTED]

[Redacted text block]

2.1.2.5.1.1.1 Functional Definition (C.2.5.1.1.1)

[Redacted text block]

[Redacted text block]

[REDACTED]

2.1.2.5.1.1.2 Standards (C.2.5.1.1.2) [RIN: MTR0128-DN]

[REDACTED] IaaS will comply with the following standards:

1. NIST:
 10. NIST SP 800-145 "The NIST Definition of Cloud Computing," September 2011.
 11. NIST SP 500-292 "NIST Cloud Computing Reference Architecture," September 2011.
 12. NIST SP 800-53 (rev.4) "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013. [REDACTED] Federal Cloud is FedRAMP compliant, however the current compliance is based upon NIST800-53 rev3 controls. CTI/QTS is in the process of upgrading from NIST800-53 rev3 controls to rev4 controls.
 13. NIST SP 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," April 2010. CTI and our team members are aware of this specification and has integrated aspects of this publication where appropriate and necessary to meet FedRAMP security control mechanisms.
 14. NIST SP 800-46 (rev.1) "Guide to Enterprise Telework and Remote Access Security." CTI [REDACTED] is aware of this specification and has integrated aspects of this publication where appropriate and necessary to meet FedRAMP security control mechanisms around remote accessibility for the CTI [REDACTED] Federal Cloud.
 15. NIST SP 800-171 "Protecting Controlled Unclassified Information in the Nonfederal Information Systems and Organizations," June 2015. CTI [REDACTED] is aware of this specification and has integrated aspects of this publication where appropriate and necessary to meet FedRAMP security control mechanisms.

2. **ITIL: ITILv3.** CTI [REDACTED] as an organization that adheres strictly to the IT Infrastructure Library (ITIL) framework – with change management and incident management for exceptional services, we too are constantly assessing all aspects of our own organization practices and identifying places for improvement. From our own data center technology and solutions to our product delivery, we are continually improving our efficiencies and scaling to support the changing needs of our customers. We pride ourselves on our own agility and quick response to change and strive for sustainability across all of our people, processes and facilities.

3. **SNMP: SNMPv3.** CTI [REDACTED] fully supports SNMPv3.
4. **FedRAMP TIC Overlay;** this specification is currently in DRAFT form and is under evaluation by CTI [REDACTED] to determine whether the requirements can be integrated into our current cloud offer. We currently see no issue with stating that we will comply with this specification.

5. **OMB M-06-16 "Protection of Sensitive Agency Information,"** 23 June 2006. CTI [REDACTED] is aware of this specification and has integrated aspects of this publication where appropriate and necessary to meet FedRAMP security control mechanisms.

6. **ISO 17203 "Open Virtualization Format Specification."** CTI [REDACTED] is aware of this specification and has integrated aspects of this publication where possible and appropriate.

7. **FIPS 140-2, Security Requirements for Cryptographic Modules.** CTI [REDACTED] is aware of this specification and has integrated aspects of this publication where appropriate and necessary to meet FedRAMP security control mechanisms.

8. CTI/QTS will work with agencies to provide application layer encryption in accordance with the FIPS 197 requirements to ensure that all data in motion and at rest is secure end-to-end. If additional encryption is then required strictly in the storage components of the solution, CTI [REDACTED] will provide encrypted storage solutions for agency as well.
9. DOD STD-5015.2 V3, Electronic Records Management Software Applications Design Criteria Standard. CTI [REDACTED] is aware of this specification and has integrated aspects of this publication where possible and appropriate.
10. NARA Bulletin 2008-05, July 31, 2008, Guidance concerning the use of e-mail archiving applications to store e-mails. CTI [REDACTED] is aware of this specification and has integrated aspects of this publication where possible and appropriate.
11. As an Infrastructure-as-a-Service offering, the CTI [REDACTED] Team complies with this.
12. NARA Bulletin 2010-05, September 08, 2010, Guidance on Managing Records in Cloud Computing Environments. CTI [REDACTED] is aware of this specification. This specification is largely out of scope for IaaS cloud services, however the CTI Team will comply.

2.1.2.5.1.1.3 Connectivity to Cloud Data Center (C.2.5.1.1.3)

[REDACTED] CTI [REDACTED] operates carrier-neutral data center facilities. This means that customers can select their communications service providers from hundreds of carriers, Internet Service Providers, dark fiber and satellite companies to meet their transport requirements. Selecting a provider from such a broad list of options gives customers exceptional route diversity and pricing options, as well as different Service Level Agreements and installation schedules. Customers who need very high amounts of bandwidth to conduct their business efficiently will never have to worry about running out of capacity [REDACTED]. Similarly, customers who require

exceedingly high communications security have the benefits of selecting from physically diverse routes between their ends points and dark fiber that is not shared with any other users. [REDACTED]

[REDACTED]

2.1.2.5.1.1.4 Technical Capabilities (C.2.5.1.1.4) [RIN: MTR0091-DN, MTR0123-DN]

[REDACTED] CTI [REDACTED] will support the basic capabilities for Private Cloud IaaS defined in NIST SP 800-145 as specified in the TO. [REDACTED] CTI [REDACTED] assumes that the capabilities listed below are mandatory unless marked optional:

CTI [REDACTED] understands and complies with the NS/EP, Federal recovery prioritization including having Local Emergency Response Action Plans for every individual data center and environments within each data center [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] CTI [REDACTED] will work with agencies ordering networks from our EIS solution to ensure that any connectivity ordered into their Cloud platform hosted with on EIS or any connectivity between the Agency and other sites ordered from our EIS solution will have the appropriate prioritizations set in our systems to flag any tickets or issues with the network has the highest priority required. Likewise the IaaS platform order and resources therein will also be marked to NS/EP federal standards to prioritize delivery, recovery, and scalability therein.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] The overall goal allows its clients to have the fastest, most flexible, redundant and scalable routes, eliminating the bottlenecks and the single points of failure.

2. Cloud Data Center Security:

[REDACTED]

High Availability - A highly resilient MPLS nationwide backbone network with protected, on-ramp access points that leverage DWDM technology establishes reliable bandwidth connections between sites.

Dedicated and Secure - Dedicated, high bandwidth connectivity with MPLS encapsulation ensures a secure end-to-end connection to protect your data.

Scalable Bandwidth - Ability to easily increase bandwidth in 10 Mbps increments, up to a maximum of 1Gbps per endpoint, allows you to expand your bandwidth with your business needs.

Flexible Network Configurations - Supports multiple network topologies, point-to-point, point-to-multipoint or any-to-any, using either Layer 2 or Layer 3 protocols, enabling the flexibility to design your connectivity solution to serve your particular needs and to route your data optimally.

Cost-effective, Bundled Solution - All inclusive, bundled offer is a simpler, more cost-effective alternative to traditional private line services. Or Agencies with high end security needs can also order Agency dedicated solutions in alignment with the Data Center to Agency Site solutions referenced in 2. b)

Fully Managed, End-to-End - End-to-end, proactive monitoring and management, 24x7x365, provides a fully managed solution.

[Redacted content]

[REDACTED]

[REDACTED]

[REDACTED]

Predictable performance provided by Ethernet circuits that travel over a single carrier's infrastructure, and data that follows a more consistent path than Internet traffic.

Customer data that is sent over a private connection and never intermingled with anyone else's traffic.

Bandwidth that can easily scale up or down as needed.

Redundant connections available for lower and higher bandwidth connections.

A single point of contact for all billing, service orders, provisioning, and issues.

Features include:

A dedicate, private, point-to-point EVC.

Availability of protected and unprotected options.

Bandwith options between 50 Mbps and 10 Gbps.

Choice of dedicated or shared ports:

1 Gbps and 10 Gbps connections are available only on dedicated ports.

For bandwidth of less than 1 Gbps, shared and dedicated port options are available.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[Redacted content]

[REDACTED]

[REDACTED]

[REDACTED]

4. Virtualiz Virtualized Elastic Computing infrastructure:

Within the vCGS platform there are two classes-of-services:

Dedicated Cloud class of service provides a single-tenant private cloud with dedicated computing servers, layer-2 network isolation for workload traffic, dedicated storage volumes, and a dedicated cloud management instance.

Infrastructure capacity may be allocated to a single virtual datacenter or multiple datacenters at your option.

Virtual Private Cloud class of service provides a multi-tenant virtual private cloud with logically isolated resources on shared physical infrastructure, configured as a single virtual datacenter with networking resources.

Each class of service includes the capability to access these objects and manage them to align with different consumption and administration models:

Virtual Datacenters (VDCs) in both classes of service will be set up with an internal VDC network and edge gateway with optional NAT-routed network. Virtual Machines (VMs) are first-class objects in vCloud Government Service interactions; they may be created and managed individually. VMware vSphere® vApps™ will be visible along with their VM associations on the vCloud Hybrid Service Console, but can be created or managed only through VMware® vCloud Director®. VMs can be added and deleted at will or scaled up or down within the Agencies Dedicated Cloud or Virtual Private Cloud Resource Pool instance at will within the vCloud console. Additional resources can be ordered at any time to increase the computer, network or storage capacity of an Agency's Dedicated Cloud or Virtual Private Cloud resources at any time.

Networks may be managed through the vCloud Director Console for edge gateway configuration and common use cases such as NAT mappings, firewall rules and VM to network assignment.

Advanced settings configuration and management such as VPN setup, load balancing and network creation can be done through vCloud Director.

Included in an Agencies Dedicated Cloud or Virtual Private Cloud resources are Compute, Network, and Storage elements. These resources can be increased or decreased by the Agency at any time. If the storage within the IaaS infrastructure is not sufficient to meet the agencies needs for any reason CTI [REDACTED] can work with any agency on off site storage, disc back up solutions on or off site, and tape back up on or offsite for any negotiated duration of time.

5. Virtual Machines (VMs).
6. Network Storage.
7. Server Hosting
 - a) Private-facing Internal Web Hosting
 - b) Public-facing External Web Hosting

Public and Private facing Web Hosting solutions are traditionally determined by the application creation and then the resources who have access to those applications. Agencies have controls from the Network layers all the way through

the Application layers to grant access to the user groups that require access to the solution Hosted in the vCGS IaaS structure. Number 2 above talks in detail about some of the multiple types of access from Layer 1, 2, and 3 public or private that agencies could connect to their vCGS environment. An agency requiring both a private facing and a public facing web solution can actually purchase two separate resource pools within IaaS to add separation at the customer hypervisor level of the environments rather than Agency administrators worrying about it at the VM level within a single resource pool.

16. Private-facing Internal Web Hosting

17. Public-facing External Web Hosting

8. Backup and Restore agency data. [REDACTED] CTI [REDACTED] can support a variety of backup/restore options for agency data.
9. On-demand self-service IaaS provisioning, configuration management, topology management, security management, activation and deactivation via portal scripting language or API with role based access control for portal login which is OMB M-11-11 compliant. Supported via the CTI [REDACTED] Cloud Portal.
10. Visibility into usage of measured/metered (usage-based) service. Visibility into usage statistics is supported via the CTI [REDACTED] cloud console/portal.
11. Allow users to have VMs with their own private IP address blocks. Supported via the CTI [REDACTED] Cloud Portal.
12. Support bulk import and export of VM per ISO 17203.
13. Allow users access to log events such as resource provisioning and de-provisioning, VM start and stop, and account changes, for at least 60 days. Supported via the CTI [REDACTED] Cloud Portal.
14. (Optional) Allow users to place metadata tags on provisioned resources and to run reports based on them, which is useful for internal show-back or chargeback.
15. Support cost control measures such as quotas (limits on what a user can provision) and leases (time-limited provisioning of resources). Cost control measures are inherently built into the CTI [REDACTED] Reservation Pool model for allocation of cloud services.

16. Support with 24x7 customer service, via phone, email and chat. Supported via the CTI/QTS Team's Operations Support Center (OSC) which is available to resolve customer issues 24x7x365.
17. [REDACTED] CTI [REDACTED] understands that an agency will retain exclusive ownership over all of its data in the cloud. [REDACTED] CTI [REDACTED] will provide tools to allow the client agency to fully retrieve its data in the original or a mutually agreed-upon format.
18. Cloud resources, particularly the data at rest, must be located within the U.S. or the jurisdiction identified in the TO to allow electronic discovery (eDiscovery) of identification, collection, processing, forensic analysis, auditing, and production of Electronically Stored Information (ESI) required in the discovery phase of litigation. This shall also include government access to the contractor's cloud data center facilities, installations, technical capabilities, operations, documentation, records, and databases if required. All CTI [REDACTED] Cloud nodes are located within the Continental United States (CONUS); specifically in FedRAMP-compliant cloud nodes in Richmond, VA and Atlanta, GA.
19. [REDACTED] CTI [REDACTED] will provide Disaster Recovery (DR) and Continuity of Operations (COOP) per agency-specific requirements in the TO subject to design review.
20. vCloud Connector will support migration of VMs, vApps, and templates between the vCloud Government Service and other vSphere or vCloud Director environments such as datacenters or vCloud Hybrid Service evaluation environments. Export, transport, and import may use vCloud Connector or Open Virtual Machine Format (OVF). These migration capabilities support onboarding to the vCloud Government Service, export from the Service, and synchronization of templates between the vCloud Government Service and your on-premises data centers.

In addition to the basic network-based copy operation of VMs, vApps, and templates between vSphere, vCloud Director, vCloud SP, and vCloud Government Service, vCloud Connector also supports the following use cases:

Extend your network from your private vSphere and vCloud Director Environments to vCloud Government Service so you can migrate VMs or vApps to vCloud Government Service while retaining the same IP and MAC address. This allows those VMs or vApps to communicate with other VMs or vApps in the private vSphere or vCloud Director Environments.

Synchronize your vCloud Government Service catalog with your private vSphere folder or vCloud Director Catalog so that all authorized users of your private vSphere or vCloud Director and vCloud Government Service use the same templates.

2.1.2.5.1.1.4.1 TECHNICAL CAPABILITIES OF PRIVATE CLOUD AND COMMUNITY CLOUD (C.2.5.1.1.4.1)

■ CTI ■ will support the following technical capabilities for Data Center Augmentation with Common ITSM. We assume the following capabilities are mandatory unless marked optional:

1. Ability to manage both cloud virtual resources and the agency data center's virtual resources with interoperable monitoring and control capabilities.
2. ■ CTI ■'s management platform shall include a visual indicator of which resources are in the cloud and which are premises resources.
3. (Optional) Ability to integrate with agency's data center management platform. This requirement is highly dependent upon the specific management platform. Therefore, additional details are required to further evaluate this requirement.

2.1.2.5.1.1.4.2 TECHNICAL CAPABILITIES OF DATA CENTER AUGMENTATION WITH COMMON INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM) (C.2.5.1.1.4.2)

CTI [REDACTED] will support the following technical capabilities for Data Center Augmentation with Common ITSM. The following capabilities are mandatory unless marked optional:

1. Ability to manage both cloud virtual resources and the agency data center's virtual resources with interoperable monitoring and control capabilities. The CTI [REDACTED] Federal Cloud portal can be used to manage virtualized resources within [REDACTED] CTI [REDACTED]'s Federal Cloud. This portal is not extendable to virtualized resources within a 3rd-party data center including Agency data centers. Additional 3rd-party cloud orchestration tools can be used for this purpose.
2. The contractor's management platform shall include a visual indicator of which resources are in the cloud and which are premises resources. The CTI [REDACTED] Federal Cloud portal can be used to indicate existing resources within the CTI [REDACTED] Federal Cloud only.
3. (Optional) Ability to integrate with agency's data center management platform. This requirement is highly dependent upon the specific management platform. Therefore, additional details are required to further evaluate this requirement.

2.1.2.5.1.2 Features (C.2.5.1.2)

CTI [REDACTED] assumes the following features are mandatory unless marked optional:

1. (Optional) "Bare metal" physical servers: Ability to have "bare metal" physical servers on a dynamic basis with provisioning times of two hours or less. This capability may be required for (a) a large-scale database requiring an incremental storage capacity, or (b) specialized network equipment that may not be available in the cloud, or (c) software that cannot be licensed on virtualized servers, or (d) legacy equipment that cannot be virtualized, or (e) agencies that plan to move into collocation first and then gradually migrate into the provider's cloud. CTI [REDACTED] can support requirements for "bare metal" physical servers with

large-scale databases and specialized network equipment as a dedicated private cloud deployment. These requirements cannot be satisfied using the current Federal community cloud. For requirements involving the deployment of software that cannot be virtualized and/or legacy equipment that cannot be virtualized, CTI [REDACTED] can provide dedicated Collocated Hosting Services. CTI [REDACTED] can support long-term architectural evolution that involves the migration of collocated workloads over time into a virtualized cloud environment.

2. Data management and analytics: [REDACTED] CTI [REDACTED]'s capability shall complement and extend log management and analysis services and other data center management services, per agency-specific requirements in the TO.

2.1.2.5.1.3 Interfaces (C.2.5.1.3)

[REDACTED] CTI [REDACTED] will support the interfaces identified in the TO as long as they adhere to the standards stipulated with the GSA EIS solicitation.

2.1.2.5.1.4 Performance Metrics (C.5.1.4)

The performance levels and AQL of KPIs for CTI's IaaS cloud service are defined below. In addition, CTI [REDACTED] will meet service level objectives for performance, privacy, security and support as specified in the TO.

2.1.2.5.1.4.1 Cloud Data Center (C.5.1.4.1)

[REDACTED] CTI [REDACTED] will meet service level objectives for performance, privacy, security and support as specified in the TO.

KPI	Service Level	Performance Standard (Threshold)	AQL	How Measured
-----	---------------	----------------------------------	-----	--------------

Availability (IaaS cloud service)	Routine	99.95%	≥ 99.95%	See Note 1
	Without Dispatch	4 hours	≤ 4 hours	
Time to Restore (TTR)	With Dispatch	8 hours	≤ 8 hours	

Table 16: Cloud Data Center Performance Standards

Notes:

- IaaS cloud service Infrastructure availability is calculated as a percentage of the total reporting interval time that the IaaS infrastructure is operationally available to the agency. Availability is computed by the standard formula:

$$Av(IaaS) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

The scheduled maintenance windows are excluded from the availability calculation.

CTI agrees to provide availability to the Federal Cloud infrastructure subject to the following SLA:

Internet Access Guarantee. Except in the event of Facilities Maintenance, Customer Maintenance, and Force Majeure conditions, CTI shall have the contracted Internet access available for the Customer to transmit information to, and receive information from the Internet 99.999% of the time during contracted term.

Internet Access Remedy. In the event CTI fails to provide the level of service provided in the Internet Access Guarantee, customer shall receive the applicable remedy (“Service Level Credit”) described below. The Internet Access Guarantee is measured on a calendar month basis.

LENGTH OF OUTAGE	SERVICE LEVEL CREDIT
------------------	----------------------

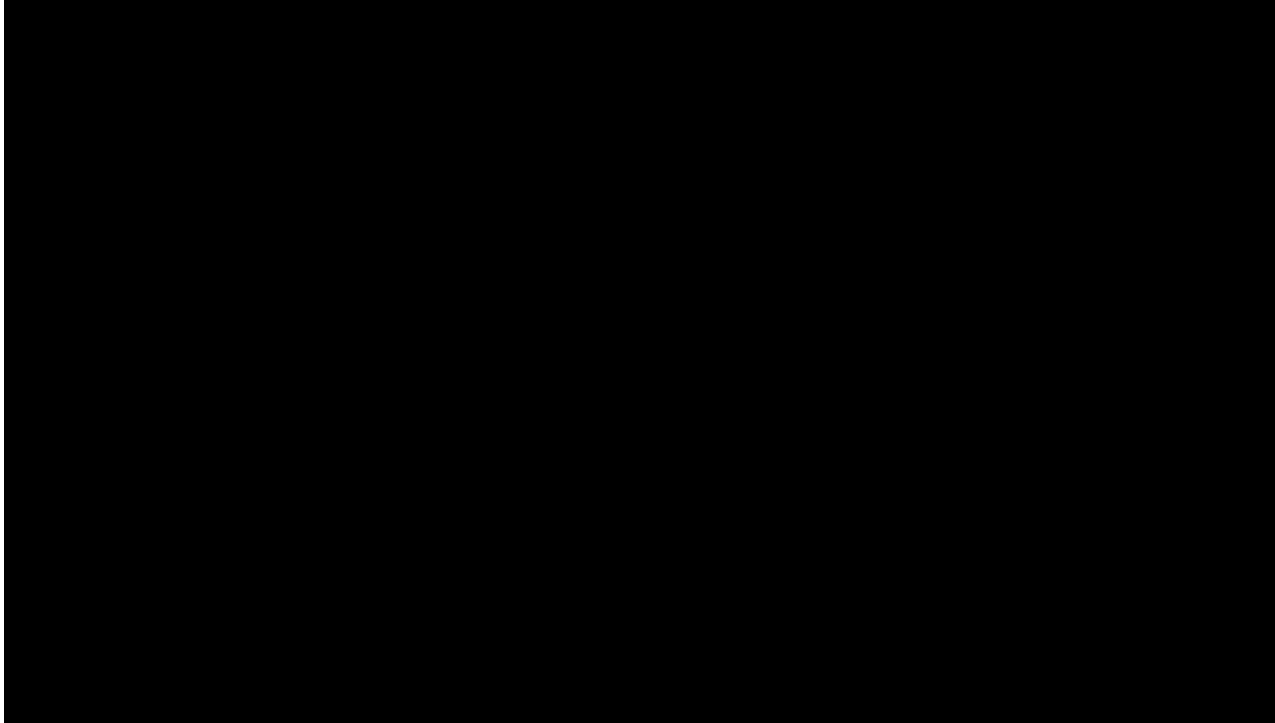


Table 17: Cloud Data Service Length of Outage vs Service Level Credit

Cloud Infrastructure Availability Guarantee. Except in the event of Facilities Maintenance, Customer Maintenance or Force Majeure conditions, CTI [REDACTED] shall make the infrastructure devices configured with high availability available for the Customer 99.999% of the time (“Cloud Infrastructure Availability Guarantee”). Infrastructure includes all hardware and equipment that make up the core IaaS environment. It does not include OS Layer and above and excludes vMotion time.

Cloud Infrastructure Availability Remedy. In the event that CTI [REDACTED] Members fails to provide the level of service provided in the Cloud Infrastructure Availability Guarantee, Customer shall receive the applicable Service Level Credit described below. The Cloud Infrastructure Availability Guarantee is measured on a calendar month basis.

2.1.2.5.1.4.2 Transport to Cloud Data Center (C.5.1.4.2)

The Performance Metrics (KPIs for availability and latency) for IaaS Transport to the CTI Team's IaaS Data Center (see Section 2.1.2.5.1.1.3 Connectivity) will comply with the individual EIS transport service's performance metrics used, as follows:

1. When both agency WAN and Cloud Infrastructure are from the same EIS contractor, the IaaS contractor will comply with the:

18. KPIs for VPN Service (VPNS), as defined in Section C.2.1.1.
19. KPIs for Ethernet Service (EthS), as defined in Section C.2.1.2.
20. KPIs for MTIPS, as defined in Section C.2.8.6.
21. KPIs for Private Line Service (PLS), as defined in Section C.2.1.4.
22. KPIs for IPS, as defined in Section C.2.1.7.

2. *When agency WAN and Cloud Infrastructure are from the different EIS contractors, the agency's WAN EIS contractor will comply with the:*

23. KPIs for MTIPS, as defined in Section C.2.8.6.
24. KPIs for Private Line Service (PLS), as defined in Section C.2.1.4.

2.1.2.5.2 Platform as a Service (C.2.5.2)

No bid.

2.1.2.5.3 Software as a Service (C.2.5.3)

No bid.

2.1.2.5.4 Content Delivery Network Services (C.2.5.4)

No bid.

2.1.2.6 Wireless Services (C.2.6)

No bid.

2.1.2.7 Commercial Satellite Communications Services (C.2.7)

No bid.

2.1.2.8 Managed Services (C.2.8)

2.1.2.8.1 Managed Network Service* (C.2.8.1)

**Mandatory Service, answered above in Section 2.1.1.5*

2.1.2.8.2 Web Conferencing Service (C.2.8.2)

No bid.

2.1.2.8.3 Unified Communications Service (C.2.8.3)

No bid.

2.1.2.8.4 Managed Trusted Internet Protocol Service (C.2.8.4)

No bid.

2.1.2.8.5 Managed Security Services (C.2.8.5)

No bid.

2.1.2.8.6 Managed Mobility Service (C.2.8.6)

No bid.

2.1.2.8.7 Audio conferencing (C.2.8.7) [RIN: MTR0047-DN]

CTI's Media Application Server (MAS) application provides the meet me and ad hoc conferencing functions as well as announcements and tones.

2.1.2.8.7.1 Service Description (C.2.8.7.1)

CTI's solution for ACS is an application layer service that requires an underlying transport to connect to the audio conference bridge application platform.

CTI's solution for Audio Conferencing Service (ACS) primarily includes a proprietary application server solution in redundant and secure carrier grade datacenters. Access to ACS is available via PSTN thru two secure carriers in a redundant environment. Most ACS user configurations include both a primary and a secondary dial in number. Access to ACS is also available via IP network for endpoints using non-traditional voice access.

The solution is accessible via single-line telephones, multiline key telephone systems, conference-room audio equipment, PBX, Centrex, and Workstation/PC based soft-phone.

CTI's solution for ACS can support an audio conference call from a few participants to a few thousand participants, such as an Agency-wide broadcast with audio feedback for questions and answers from callers.

The diagram below shows the connectivity from multiple participants to an ACS audio conferencing bridge, which supports the audio conference.



Figure 14: Audio Conferencing Service Description

2.1.2.8.7.1.1 Functional Definition (C.2.8.7.1.1)

2.1.2.8.7.1.2 CTI's solution for ACS is a service that facilitates a call

between three or more people in two or more locations that allows participants to converse with each other. The service allows participants to engage in either operator assisted or non-assisted multi-point audio conference calls. Audio conferencing can be initiated from Government sites using single-line telephones, multiline key telephone systems, conference-room audio equipment, PBX, Centrex, and Workstation/PC based soft-phone; and, from non-government sites while on travel or working remotely. Standards (C.2.8.7.1.2) [RIN: MTR2242-DN]

Audio Conferencing Service will comply with the following standards as applicable:

1. ANSI T1.101 for T1.
2. ANSI T1.607 and 610 for ISDN.
3. ANSI SS7, and enhanced SS7 standards for interworking (e.g., address translation) between circuit-switched network and IP network.
4. Telcordia Notes on the Networks (SR-TSV-2275).
5. IETF RFC 3661 through 3665 for SIP (Session Initiation Protocol) .
6. IETF RFC 3435 for MGCP (Media Control Gateway Protocol).
7. ITU-TSS H.323/225/245/248 (enhanced for VoIP).

CTI will comply with new versions, amendments, and modifications made to the documents and standards listed above.

2.1.2.8.7.1.3 Connectivity (C.2.8.7.1.3)

Audio Conferencing Service will connect to and interoperate with:

1. Government specified locations, such as single-line telephones, multiline key telephone systems, conference-room audio equipment, PBX, Centrex, and Workstation/PC based soft-phone.
2. PSTN.
3. Internet.
4. CTI's network and all other contractors' networks for:
 - a. Circuit-switched services (for TDM landline and Cellular voice service).
 - b. IP service (for VoIP).

2.1.2.8.7.1.4 Technical Capabilities (C.2.8.7.1.4) [RIN: MTC0017-DI, MTC0018-DI, MTC0019-DI, MTC0020-DI, MTC0021-DI]

The following Audio Conferencing Service capabilities are mandatory unless marked optional:

1. **Multi-point Bridging Capability.** The bridging capability will allow selective two-way or one-way conversations between conferencing ports; i.e., it will allow a subset of conferees to participate in a two-way conference while the remaining conferees are listeners only. During the conduct of a multi-point conference, the addition of a party to, or the deletion of a party from, the conference will be indicated by a tone or by a verbal announcement.
2. **Conference Set-up Capability.** CTI will provide the following conference set-up support services:
 1. **User-Controlled Conference.** This capability will allow authorized users and users with a calling-card to establish a conference call by dialing a designated number to access the service. If calling card is used, all charges will be billed against the calling card. The following two automated modes of user-initiated conferencing capabilities will be supported:
 - i. **Meet-Me Conference** - This capability will allow each user to be connected in a Conference by dialing a designated number and authorization/pass code at a predetermined time or as directed by the

operator. For recurring dial in conferences, CTI will permit the participants to reuse the same dial access number and authorization/pass code and allow bookings of recurring conferences in three month increments (e.g., every Monday morning at 10:00 AM for the next three months).

- ii. **Preset Conference** - This capability will allow an authorized user to activate a previously defined conference with associated conferees by dialing an access number followed by an authorization/pass code. Once activated, the system will attempt to connect the pre-designated participants using the predefined lists. CTI will provide a report for “no shows” when the Preset Conference was not activated, showing the bridge numbers and the associated conferees.

2. **Attendant-Assisted Conference.** This capability will allow operators to establish a conference. Conferees will be able to recall an operator during a conference for immediate attention, such as general assistance or adding or dropping participants.

3. **Audio Conference Reservation System.** The audio conference reservation system will permit authorized government users to schedule audio conferences.

The reservation system will have the following capabilities:

1. A single point of contact with CTI (preferably, the Customer Service Center) to schedule reservation-based audio conferences.
2. Ability for authorized users to schedule one or more conferences by time and day of the week either as a single event or recurring event on a daily, weekly, monthly, or other periodic basis. In addition, it will be possible to schedule an emergency audio conference call within 15 minutes if bridging capacity is available.
3. The ability for authorized users to submit reservation requests up to one year in advance by phone or Email or fax or via online through Internet.
4. The ability to store and retrieve predefined conferences.
5. The ability to create printed reports with reservation confirmation and cancellation notices.
6. The reservation system will contain the following information:

-
- i. Type of conference (e.g., video, audio).
 - ii. Name of the person scheduling the conference.
 - iii. Organization of the person scheduling the conference.
 - iv. Telephone number of the person scheduling the conference.
 - v. Name of an alternate contact person.
 - vi. Telephone number of the alternate contact person.
 - vii. Name of the contact person at participating locations (attendant- assisted only).
 - viii. Telephone numbers of the contact persons participating in the conference (attendant-assisted only).
 - ix. Name, organization, telephone number, and email address of each person participating in the conference (at the user's discretion).
 - x. Locations of the persons participating in the conference (at the user's discretion).
 - xi. Date of the conference.
 - xii. Time of the conference.
 - xiii. Scheduled length of the conference.
 - xiv. Email confirmation notification to each participant with conference details (at the user's discretion).
 - xv. Authorization/billing code or calling card number.
4. **Automatic port expansion.** CTI shall provide and support automatic port expansion which will allow, without operator assistance, automatic expansion to additional ports to the conference in progress beyond the dial-in ports reserved as long as facilities are available.
 5. **Conference tones.** This capability will enable or disable conference tones when a participant enters or exit a conference.
 6. **Participant count.** CTI will provide and support audio conferencing capability that will provide a count of participants on the call in real-time such that the count is updated as participants enter or leave the conference.

-
7. **Roll call.** CTI shall provide and support an audio conferencing Roll Call capability which will enable or require the operator to conduct a roll call of participants so that all participants know who are on the conference and in real-time let everyone know who has left the conference and/or re-entered the conference.
 8. **Attendant assistance.** CTI shall provide and support attendant assistance for audio conferencing on demand at any time during an audio conference. Operator Assistance is available at any time while accessing the conferencing system by dialing 0. This includes during dialing streams. The operator is typically a defined administrator or SIP URL on the system. It could also be routed for treatment to play an announcement of some sort. Assistance in the form of file and screen sharing can also be provided with the service.
 9. **Announce late participant.** This capability will provide either the announcement of participants arriving late to the call or blocking of late participants from joining the conference based on user's instruction.
 10. **Enable and disable music on hold.** This capability will enable or disable music on hold when a participant is put on hold.
 11. **Enable and disable self-mute.** This capability will provide self-mute if this capability is not available on their phone.
 12. **Guaranteed duration of dial-in call.** This capability will provide guaranteed duration of dial-in call and will allow participants to hang up at any time and rejoin the conference later.
 13. **Listen-only broadcast mode.** This capability will allow listen-only broadcast mode.
 14. **Mixed mode.** This capability will provide mixed mode, i.e., both listen-only and interactive modes.
 15. **Audio Conferencing Service.** This capability will provide users with the following service intervals and will be available 24 hours a day, seven days a week:

1. Schedule a non-recurring conference within 30 minutes after the advance reservation request, provided that the bridging capacity and the other required network support functions are available.
2. When bridging capacity and other required network support functions are available, requests for a delay in the scheduled termination time of a conference that is already in progress will be granted if the request is made at least 20 minutes before the scheduled terminating time of the conference.
3. Permit ACS users to cancel an audio conference up to 30 minutes before the scheduled start time of the conference without incurring any charge for the canceled conference.

2.1.2.8.7.2 Features (C.2.8.7.2) [RIN: MTC0022-DI, MTC0023-DI, MTC0024-DI, MTC0025-DI, MTC0028-DI, MTR0072-DN, MTR2246-DN]

The following Audio Conferencing Service features are mandatory unless marked optional. In addition, any other features available commercially are included in the scope of the contract.

1. Audio recording of call. CTI will allow recording of conference call into a storage-media (e.g., disc or cassette tape or USB device) for later replay.
2. Access Controlled Call. CTI will allow the conference leader to prevent operator from monitoring the call as well as additional/late participants from joining the call
3. Language translation. CTI will provide language translation to English from other languages (e.g., Spanish) for transcription of pre-recorded audio conference.
4. Moderator led questions and answers. CTI will provide conference moderator led questions and answers only.
5. Participant list report. CTI will provide a report of all participants in the conference.
6. Password screening. CTI will screen password for joining a conference to authorized participants only.
7. Replay of pre-recorded audio conference. CTI will allow, under password protection, replaying of pre-recorded audio conference at a later time and will

allow remote control of the recording with keypad access to functions like pause, rewind, and fast-forward.

8. Transcription of pre-recorded audio call. CTI will provide transcription of pre-recorded audio call.
9. Temporary blocking of ports. CTI will allow temporarily blocking audio conference ports in order to remove a sub-set of participants/users from the conference.
10. Secured Audio Conference. CTI will support voice conferencing capability for sensitive voice conferences with end-user encryption to support discussions of a CUI nature between multiple locations with protection from unauthorized interception (i.e., eavesdropping).
11. Operator Dial-out. CTI shall provide and support the capability to add a participant to a conference via an outbound call from the conference bridge initiated by the conference attendant.
12. Host dial-out. CTI shall provide and support the capability to add a participant to a conference via an outbound call from the conference bridge initiated by the conference host. This capability can be individual calls or group calls to add a particular group to the session. These calls can be made without disruption of the session and occurs in the background, with each joining participant annotated on the session list which is viewable by all participants.
13. Executive Conference. CTI shall provide and support professional moderator assistance with control of conference attendant functions.
14. International global meet. CTI shall provide and support International global meet service that provides in-country local access, which is a non-North American toll number assigned to a specific country and bridge.
15. Host controls. Host controls. CTI shall provide and support the capability to allow the conference host to control conference attendant functions.
16. Audio recording of a conference bridge is accomplished by dialing *9 to start/stop recording of the conference.

17. A Conference host can lock the bridge by dialing *4, and new bridge pin can be issued by dialing 52 by the conference host. Also, the host can terminate a bridge by dialing 11 and reissuing a new pin to only the distribution of people they want to join a conference.

18. Encryption of MAS audio is accomplished using TLS/SRTP

19. Operator dialout is supported in the conference system.

20. International global meet is supported using local dial features.

21. Conference hosts have the following control commands available:

Mute Options

*6 mute self, *7 unmute self, ## mute conference, 88 mute each conference party, 99 unmute the conference

Additional Commands

*3 toggle entry/exit notification, *# count participants, *4 lock conference, *5 unlock conference, *8 conference continuation, 11 kill conference, *0 assume chair, *9 start/stop recording, 51 toggle fast start, 52 change pin, 53 change entry/exit notification, 54 save settings, 55 toggle IM notification

Audio Emoticons

*1 Enable/Disable, 2 (0-9) to play

Help Options

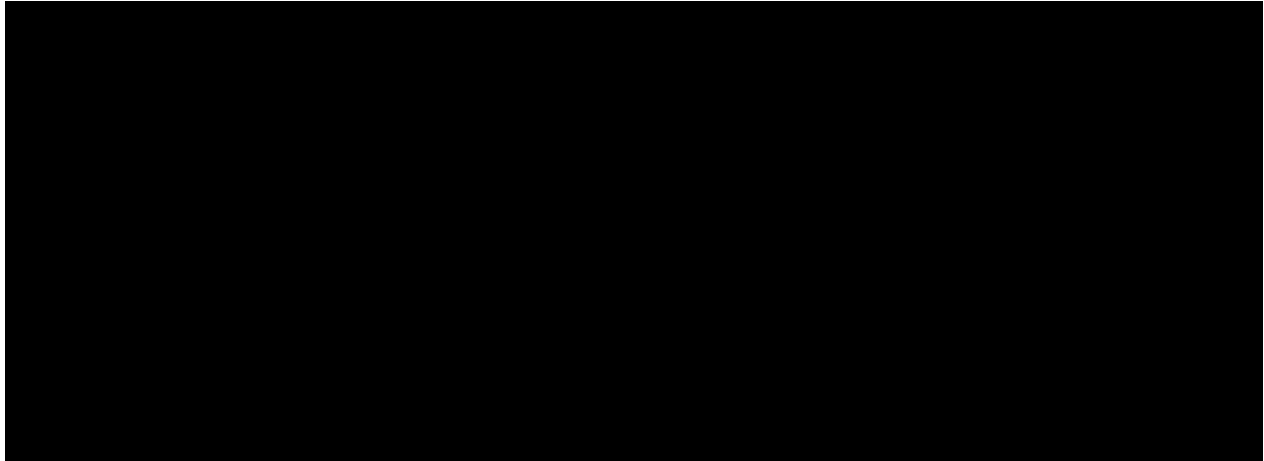
00 call an operator, ** audio help

2.1.2.8.7.3 Interfaces (C.2.8.7.3)

CTI will support audio connection to the conference-bridge from services such as landline voice service (VoIP, TDM) and cellular voice service.

2.1.2.8.7.4 Performance Metrics (C.2.8.7.4) [RIN: MTR0052-DN]

CTI will meet the required ACS Performance standards as listed below.



2.1.2.8.8 Video Teleconferencing (C.2.8.8) [RIN: MTR0156-DN, MTR2243-DN]

No bid.

2.1.2.8.9 DHS Intrusion Prevention Security Service (C.2.8.9)

No bid.

2.1.2.9 Access Arrangements* (C.2.9)

**Mandatory Service, answered above in Section 2.1.1.4*

2.1.2.10 Service Related Equipment (C.2.10)

When identified in a TO, CTI will provide 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. CTI will also provide hardware and materials that are incidental to the installation, operation and maintenance of EIS services.

Unless otherwise specifically agreed to by the government, all equipment (hardware, firmware, and software) needed on CTI's side of the demarcation to provide a service is part of the service and will not be separately priced as SRE.

All equipment provided to the government under this contract will be new and not previously used or refurbished.

2.1.2.10.1 Definition and Online Catalog Requirement

SRE refers to separately identifiable and separately priced hardware, firmware, and software components, along with the installation, maintenance, relocation and/or removal associated with an EIS service.

CTI will develop and maintain an online catalog of SRE offerings and pricing in accordance with the requirements specified in Section B.1.3 in the GSA EIS solicitation. CTI's SRE Catalog will contain the data elements defined in this section. In addition, we list, where available, the month and year of model introduction, and provide references to this information on our websites, or indicate how to find this information on the manufacturer's website. If the model introduction date is unavailable, or is an estimate, then we will indicate this in our catalog.

2.1.2.10.2 Warranty Service (C.2.10.1)

CTI will provide, 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 this contract, including all equipment supplied, installed, and integrated by CTI. The equipment warranty will provide for hardware repairs and the distribution of updated software to all users who ordered the hardware or software under this contract. CTI will provide warranty information associated with each product and service delivered to the GSA CO or OCO upon request.

CTI will repair or replace malfunctioning equipment covered by warranty within five (5) business days or as specified in the TO. CTI will provide the government with a point of contact for the warranty who will be available from 7AM – 7PM local time, or for a longer period if specified in the TO. The warranty will begin at the time that the SRE is accepted.

2.1.2.10.3 Range of SRE Products Provided

CTI provides a wide range of SRE products in installation and maintenance, including:

- Connectors – Data connectors, D-type connectors, Fiber adapters, Fiber connectors, Patch panels, Power connectors, RF coaxial adaptors, and RF Coaxial connectors
- Cables – External cable, Fiber cable, General wire and braiding, Industrial wire and cable, Patchcords and assemblies, Power cable, RF coaxial cable, and Twisted pair cable
- Trunk and Conduit – All-purpose conduit, Aluminum trunking, Fiber ducting, Floor boxes, Industrial trunking and conduit, PVC conduit, Stainless steel trunking and conduit, Steel trunking and conduit, and steel trunking and conduit
- Steelworks – Basket mesh, Basket tray, Brackets, Cable ladder, Cable trays, Channel sections, Fixings and fittings, Supports, Cable and Pipe Supports
- Conduit, Panel and Accessories – 19” Cabinets, Cabins and base stations, Digital distribution frames, Enclosures, ETSI racks, Optical distribution frames, Patch panels, Server cabinets, Streetside cabinets, Trackside cabinets

- Active Equipment – Converters, Filters, Hubs, Multiplexers, Network termination equipment (NTEs), Power distribution units (PDUs), Remote access, Remote dialers, Routers, Switches, Test equipment, Transceivers



Figure 15: Service Related Equipment

2.1.2.10.4 Sourcing Partnership

[Redacted content]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.1.2.11 Service Related Labor (C.2.11) [RIN: MTR2217-DN]

CTI has included service-related labor in our pricing tables that is necessary to implement and support all of our proposed services (required and optional). Our list of labor categories implies that labor resources that will be utilized to fulfill EIS task orders have the experiences, certifications and security clearances needed to perform installations, construction, alterations, maintenance and repair for end to end solutions.

2.1.2.12 Cable and Wiring (C.2.12) [RIN: MTR0159-DN]

2.1.2.12.1 Service and Functional Description

Core Technology Inc., (CTI) is a small business global leader for cable wiring and is the top performing GSA small business in this field with a successful track record via our GSA STARS II and GRITS II contract vehicles. Additionally, our CTI has decades of experience in cable and wiring installations for CONUS and OCONUS sites through the

Seaport-E contract vehicle. CTI is exceptionally experienced in installation services for equipment necessary to provide telecommunications services and related supporting IT services.

For every TO requiring it, CTI will provide required connectivity using appropriate cabling and wiring, and related trenching, ducting, grounding, and lightning protection systems in accordance with the TO and appropriate standards.

Before any cable and wiring TO, CTI will send a seasoned and expert team to conduct a full site preparation work which will conform to applicable federal, regional and local codes and accepted industry installation and construction practices. All planned work and code compliance will be subject to OCO review and approval prior to the start of work. We provide all tools and test equipment to perform the site preparation as specified in the TO. CTI will retain ownership of the tools and test equipment unless otherwise specified in the TO. CTI expects the government to furnish facilities and utilities to CTI that already are installed at the site, including light, heat, ventilation, and power. CTI will provide temporary utilities that are not available in the work area and coordinate any disconnection of utilities. CTI will also 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. HVAC and electrical construction will be limited to new or upgraded installations necessary to support telecommunications and IT equipment. CTI will expand or modify power systems to provide appropriate environmental controls to support the installation.

CTI always provides a warranty period of at least one (1) year for the premises wiring/cabling after service acceptance.

Core Technologies, Inc. been designing and implementing large scale voice and data network infrastructure for over 12 years. This includes both new construction and large remodel projects. In each of these cases CTI takes on responsibilities tailored to each customer and project. In some cases we will do full design work for the entire system based on the customer's needs, in others we work closely with 3rd party engineers and designers to develop an integrated system as a team, and in still others we simply take the plans and install the system as designed. In all these cases, however, we believe

that constant and thoughtful communication occurs on a frequent basis amongst all stakeholders of the project.



Figure 16: Cable and Wiring (2)

Systems we have designed and installed include local and wide area networks, fiber optic and copper cable transmission systems, telephony systems, Audio Visual (VTC) and security and surveillance systems. CTI has successfully performed structured cabling and telecommunications solutions projects in value from <\$100K to >\$4M for the Nuclear Regulatory Commission, Drug Enforcement Agency, Federal Bureau of investigations,

Department of Defense, Department of Transportation, Department of Homeland Security, Federal Occupational Health, Veterans Administration, National Marine Fisheries Services, among others. Through a multi-year contract with the Drug Enforcement Agency (DEA), CTI installed telephone systems along with the associated cabling and data cabling infrastructure for thirteen (13) field offices located around the country. At any given time we were performing simultaneous installation at up to four (4) different field offices. The total value for all thirteen (13) task orders was over \$3.5 Million.



Figure 17: Cable and Wiring (4)

We have also installed VoIP phone systems and cabling installation for two locations with the Defense Contract Audit Agency (DCAA) and the cabling infrastructure to support five (5) different voice/data networks at four (4) different Federal Bureau of

Investigation (FBI) Field Offices. The FBI projects have a cumulative value of over \$6.5 million and we installed the infrastructure to support over 5,000 users.

Core Technologies has a tremendous amount of Data and Voice cabling experience that includes both copper and fiber installations. We take pride

in our cabling work and take every effort to install our cables in the cleanest and neatest manner possible. We want our customers to be impressed with the way their installed cables look, not only for aesthetic reasons but this will also make moves, adds, and changes within the telecom closet much easier. This saves time and allows us to control costs.



Figure 18: Cable and Wiring (3)

The pictures shown are from some of our previous projects, and they are included in a design manual that we have developed for all CTI cabling projects. This manual allows us to standardize our work and ensure a quality product for all of our customers.

2.1.2.12.1.1 Standards

We will follow all TIA/EIA Commercial Building Telecommunication Wiring Standards and National Electrical Code, OSHA, BICSI, and Avaya



Figure 19: Cable and Wiring (1)

regulations while performing the work. We will obtain any and all site specific local permits and comply with all building, city, county and state codes.

2.1.2.12.1.2 Connectivity

The Cable and Wiring Service will interoperate with all of the connectivity solutions within the EIS contract.

2.1.2.12.1.3 Interfaces

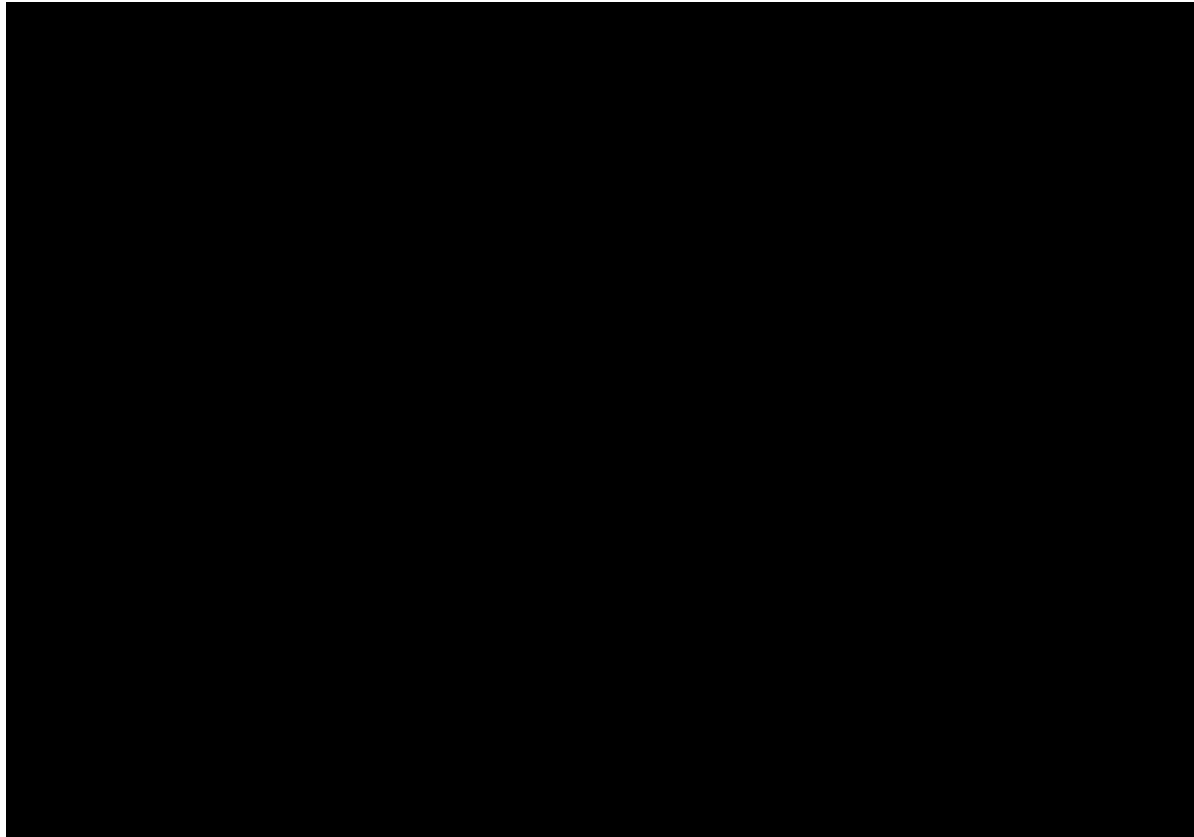
The Cable and Wiring Service will interoperate with all industry standard interfaces.

2.2 INFORMATION SECURITY (L.29.2.2)

2.3 EXTERNAL TRAFFIC ROUTING REQUIREMENT (L.29.2.3) [RIN: MTC0031-DI, MTC0004-DI, MTC0006-DI, MTC0007-DI, MTC0008-DI, MTC0009-DI, MTC0010-DI, MTR0109-DN, MTR0112-DN, MTR0121-DN, MTR0122-DN, MTR0111-KS]

CTI's architecture and services comply with security specifications as identified in the following:

- a) CTI meets service-specific requirements as defined at both the proposal and TO level. CTI also possesses the resources to adapt security needs on a post-award as-needed basis.
- b) CTI currently provides security designed for traffic of varying levels of sensitivity in our programs undertaken [REDACTED]
[REDACTED]
[REDACTED] CTI network services, information, infrastructure, and information processing resources are all shielded from security threats and system failures.
- c) CTI meets the external traffic routing requirements described in Section C.1.8.8, sub-paragraph 3, which include:
 1. CTI's methodology for identifying the offeror's participating agency traffic for each affected service shall be via IP addresses. Participating agency traffic network



3. CTI’s technical approach to notify DHS should any non-participating agency traffic (IPv4, IPv6, etc.) be redirected through DHS EINSTEIN enclaves is via email and trouble reporting and ticket tracking tools. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]


SERVICE	CAPABILITY
INCIDENT AND PROBLEM MANAGEMENT	AUTOMATICALLY DETECT AND MANAGE RECURRING INCIDENTS.
KNOWLEDGE MANAGEMENT	BRINGS KEY INFORMATION TO CUSTOMERS AND CTI SUPPORT PERSONNEL, RIGHT WHERE AND WHEN THE CUSTOMER NEEDS IT.
CHANGE MANAGEMENT	DOCUMENTS AND COORDINATES CHANGE REQUEST ACTIVITY ACROSS YOU’RE THE MNS — FROM DATA CENTERS TO DESKTOPS

RELEASE MANAGEMENT	COMBINE MULTIPLE CHANGE REQUESTS INTO A SINGLE RELEASE AND MANAGE ALL RELATED ACTIVITY IN SUPPORT OF A SUCCESSFUL RELEASE
SERVICE REQUEST MANAGEMENT	DEFINE A CATALOG OF SERVICE REQUEST TYPES THAT REFLECT WHAT SERVICES YOU OFFER TO INTERNAL OR EXTERNAL CUSTOMERS
SELF-SERVICE	CONTEXT-AWARE SELF-SERVICE APP THAT'S SOCIAL, MOBILE AND FORMLESS
ASSET MANAGEMENT	COMPLETE LIFECYCLE MANAGEMENT OF IT ASSETS, FROM PROCUREMENT TO END-OF-LIFE
SERVICE LEVEL MANAGEMENT	DEFINES, TRACKS, AND REPORTS SERVICE LEVELS
CONFIGURATION MANAGEMENT (CMDB)	SUPPORT ITSM PROCESSES WITH A SINGLE SOURCE OF REFERENCE FOR OUR IT INFRASTRUCTURE AND SERVICES
VIRTUAL CHAT	SELF-SERVICE FEATURE COMBINES A VIRTUAL AGENT AND LIVE CHAT TO IMPROVE PRODUCTIVITY, LOWER IT SUPPORT COSTS, AND BOOST CUSTOMER SATISFACTION
CUSTOM APPLICATIONS	ALLOWS CTI TO BUILD EVERYTHING FROM SIMPLE FORMS, TO TWO-WAY INTEGRATIONS, TO RICH APPLICATIONS TO MEET CUSTOMER NEEDS.
PLATFORM ADMINISTRATIONS	EASILY ALLOWS CTI TO MANAGER CUSTOMER OR ORGANIC SERVERS, LDAP AND EMAIL INTEGRATIONS, APPLICATION AND SECURITY PREFERENCES AND SECURITY LOGS

Table 19: Smart Reporting Capabilities

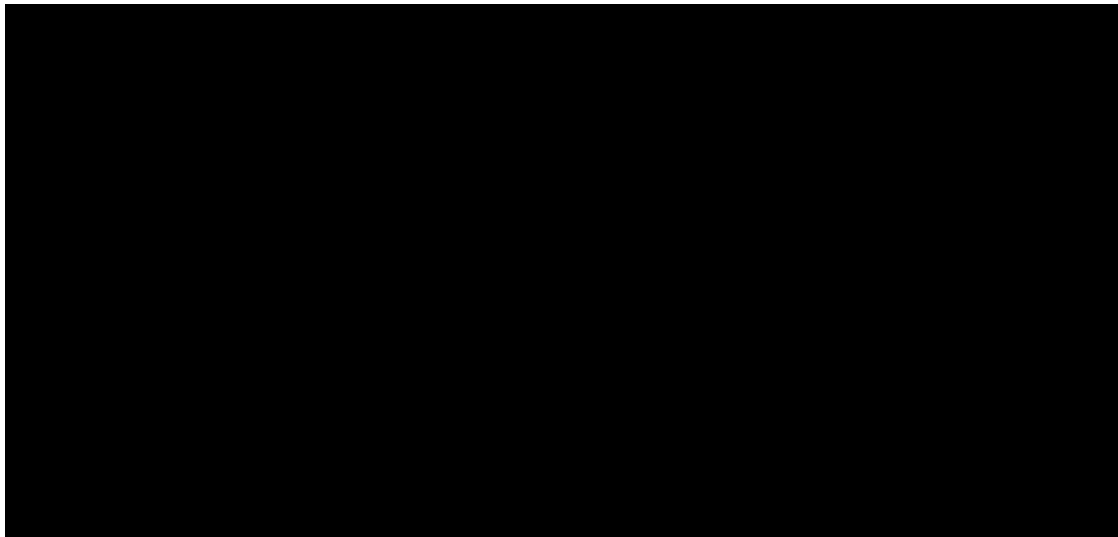
- Control mechanisms that CTI shall use to ensure that the identification and redirection of participating agency traffic is not inadvertently or maliciously bypassable shall be accomplished on CTI's network prior to purchase and deployment. Testing shall cover voice, data, and video technologies that include but are not limited to, IP VPN and voice services. Testing shall be performed at

the agency's discretion and structured in collaboration with CTI, either at CTI's headquarters or with the appropriate CTI partner depending upon type and classification of network tested. CTI will create testing environments to include sufficient equipment, software and licenses in order to replicate voice, data, video technologies and services that will be supplied to the government. Within this test environment, CTI will be able to check equipment capability, interoperability, delivery of services, and compare, prior to any delivery, any baseline changes. Baseline changes deemed to have an impact on operations, or to have an adverse effect on performance will be applied, and the unit tested on a development rack, then merged onto an integration test rack; performance tested then delivered for installation.

5. Sensing and control mechanisms CTI will use to ensure the redirection of traffic is failsafe (no disruption of participating agency services) should failures occur with DHS GFP is illustrated by the following diagram. 













[REDACTED]

7. CTI shall provide instrumentation to measure transport SLA KPIs (as if traffic passes through loopbacks in EINSTEIN Enclaves with no impact within DHS GFP being counted against the CTI's performance) by using Network Monitoring Service tools [REDACTED].

[REDACTED]

- Network traffic analysis and bandwidth monitoring that monitors interface-level network bandwidth and traffic patterns with up to one-minute granularity
- Network traffic forensics that analyze traffic patterns over months, days, or minutes by drilling down into any network element.
- [REDACTED]
- Bandwidth usage views by user, application, protocol, and IP address group to see which users, applications, protocols, or IP address groups are consuming the most bandwidth.
- Border gateway protocol and CBQoS performance statistics to view balance of network traffic across providers, and measure the effectiveness of CBQoS policies.
- [REDACTED]
- Customizable network traffic reports to create, schedule, and deliver in-depth network traffic and bandwidth reports with just a few clicks.
- Integrated fault, performance, and configuration management to seamlessly integrate with Network Performance Monitor and Network Configuration Manager
- Wireless LAN Controller traffic monitoring for WLC traffic to see which applications and clients utilize the bandwidth of your wireless network.

2.3.1 Traffic identification and routing policy (C.1.8.8(3))

CTI shall ensure that services delivered are in compliance with national policy directives that apply to the national telecommunications infrastructure.

Specific national policy requirements include, but are not limited to:

1. 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. NS/EP requirements are covered in Section G.11.
2. OMB Memorandum M-05-22 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, CTI solution must maintain functionality and shall comply with NIST SP 500-267. All systems, software, and equipment supporting the agency network and its services shall handle IPv6 in an equivalent or better way than current IPv4 capabilities, performance, and security. No systems, software, or equipment shall be deployed on the network that does not meet this requirement. Additionally, all network management shall be enabled using IPv6.
3. OMB Memorandum M-09-32, "Update on the Trusted Internet Connections Initiative," "requires all agencies to undertake immediate responsibility for executing essential agreements and updating POA&Ms to facilitate not only TIC preparations, but also due diligence for integrating the National Cyber Protection System (NCPS, operationally referred to as EINSTEIN) deployments and synchronizing with US-CERT," and OMB Memorandum M-15-01, "Fiscal year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices" requires Departments and Agencies (D/As) to enter into legally sufficient agreements with DHS relating to the deployment of EINSTEIN. DHS establishes these agreements with D/As authorizing in-line traffic inspection and modification, and such activities may include the interception, modification, use, and disclosure of D/A traffic. As such, any service offering under EIS (VPNS, Ethernet Transport, IPS, Cloud, MTIPS or otherwise) transporting Internet, Extranet, and Inter-Agency traffic shall identify and route said government traffic through a secure DHS EINSTEIN Enclave for processing by the latest generation of EINSTEIN

capabilities. CTI shall design, implement, and operate its services to achieve the required routing of traffic through (including delivery to and receipt of traffic from) DHS EINSTEIN Enclaves. Transport SLA KPIs are measured as if through loopbacks in EINSTEIN Enclaves. EINSTEIN Enclaves are strictly intermediate hops and shall not be considered end points for SLA measurement.

2.4 INTEROPERABILITY (C.1.8.6) [RIN: MTC0011-DI]

CTI shall support interoperability for given service offerings so that a user of a service from one EIS contractor shall be able to communicate with users of services from other EIS contractors with performance equivalent to that which is commercially available from CTI. Different levels of interoperability exist commercially, particularly in the area of data networking, however technical standards are such that interoperability shall be made available for any service that is currently commercially offered by one contractor and is interoperable with services of other EIS contractors. In addition, CTI shall make available any future service interoperability at no additional cost to GSA when CTI offers the interoperability for its commercially provided service. Since near full interoperability is provided via the Public Switched Telephone Network (PSTN) for circuit switched services, CTI shall support interoperability between voice services, circuit switched data service, and wireless services. CTI shall also support connectivity and interoperability for remote and mobile users as specified in the individual service descriptions.

2.5 SYSTEM SECURITY (C.1.8.7) [RIN: MTR0132-DN, MTR0133-DN, MTR0135-DN, MTR0136-DN, MTR0137-DN, MTR0138-DN, MTR0139-DN]

2.5.1 System Security Compliance Requirements (C.1.8.7.1)

In providing EIS services, CTI complies with all applicable federal and agency-specific IT security directives, standard, policies, and reporting requirements. CTI also complies with FISMA, DOD, and Intelligence Community-associated guidance and directives to

include all applicable Federal Information Processing Standards (FIPS), NIST SP 800 series guidelines, agency-specific security directives, policies and guides, and other government IT. In addition to these compliances, CTI complies will comply with all service specific security requirements identified within Section C.2 Technical Requirements, which includes both Cloud Infrastructure as a Service (IaaS), which CTI is offering, or Managed Trusted Internet Protocol Services (MTIPS), which CTI is not offering at this time.

CTI and its partners depend on information technology and the information systems to successfully carry out our business functions. The risk mitigation strategy implemented at CTI and its partners provide process (background checks, plans, policies, controlled access, etc.), physical (smart-cards, readers, hardened server cages, back-up servers, separate power supplies, SCIF's guards, cameras, intrusion alarms, man-traps, etc.) and technical (agency-specific help desk services and shared or dedicated NOCs and SOC Tier I, II and III help desk services to using BMC Remedy software that provides Incident & Problem Management, Knowledge Management, Configuration Management, Change Management, Asset Management and Service Level Management, etc.). Threats to information and information systems include environmental disruptions, human or machine errors, and purposeful attacks. Cyber-attacks on information systems today are often aggressive, disciplined, well-organized, well-funded, and in a growing number of documented cases, very sophisticated. Successful attacks on public and private sector information systems can result in serious or grave damage to the national and economic security interests of the United States. Given the significant and growing danger of these threats, CTI and our partners understand our responsibilities to federal agencies when they execute purchases or provide services under the EIS solicitation. Therefore, our requirements mandate having basic and advanced procedures in place for achieving adequate information security, and for managing information system-related security risks.

The CTI Team has multiple risk mitigation strategies in place for the GSA EIS contract to provide basic security for all network services, as well as the network management

systems and information systems and databases used to support those services. CTI's approach is a three tiered that addresses risk-related concerns at the organization level; the business process level and the information systems or network level. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The objective of the Risk Management process is to ensure both physical and The schematic is broken into five phases or tasks for Federal information and information

systems in putting together CTI's risk mitigation strategy. [REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[Redacted text block]

[Redacted text block]

- [Redacted list item]

- [Redacted list item]

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

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

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block containing multiple paragraphs of information, all obscured by black bars.]

As noted above our risk mitigation planning strategy helps CTI provide basic security for all network services, as well as the network management systems and information systems and databases used to support those services. Such security includes protecting all network services, information, CTI infrastructure, and information processing resources against threats, attacks, or failures of systems. Our risk mitigation plans are comprised of both formal and expert based mitigation. [REDACTED]

[REDACTED]

[REDACTED] As part of our overall approach the CTI risk management strategy is propagated within our organization and to business partners and contractors, some of whom may have programmatic, planning, developmental, acquisition, operational, and oversight responsibilities. Please see our Risk Mitigation Plan within the Technical Proposal response.

2.5.2 System Security Plan (SSP) (C.1.8.7.4)

As per the requirements in Section C.1.8.7.4, CTI, when delivering services under a TO, will comply with all security A&A requirements mandated by federal laws, directives and policies, including making available and documentation, physical access, and logical access needed to support this requirement.

2.5.3 Personnel Background Investigation Requirements (C.1.8.7.7) [RIN: MTC0032-DI]

All CTI personnel with access to government information that is within the security A&A scope shall perform personnel security and/or suitability checking in accordance with FAR Part 52.204-9. All CTI personnel shall successfully complete a background

investigation in accordance with Homeland Security Presidential Directive-12 (HSPD-12) Office of Management and Budget (OMB) guidance M-05-24, M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors," and as specified in agency-identified security directives and procedural guides.

2.6 TECHNICAL SUPPORT (C.1.8.9) [RIN: MTC0030-DI]

2.6.1 Customer Support Office and Technical Support (G.6.2)

CTI shall provide customer technical support as a component of each of its EIS services. CTI's CSO shall be located at our Headquarters located at 2800 Colonnades Ct., Norcross, GA 30071. This facility shall provide basic operations at contract award; CTI shall provide all customers with a main toll-free telephone number and primary email address. CTI shall have all functional areas of the CSO fully operational within 30 days of NTP. Our CSO shall perform the following services and/or facilitate the following efforts:

1. Facilitate the government's use of the contract.
2. Provide contact information for each functional area of the CSO.
3. Respond to general inquiries.
4. Provide information regarding available products and services, respond to service inquiries, and accept orders.
5. Provide training registration and scheduling information.
6. Respond to inquiries via the same method the customer used to access the CSO, unless otherwise specified by the customer.
7. Provide a main US toll-free telephone number through which all CSO functional areas can be accessed.
8. Provide the capability for non-domestic users to contact the CSO without incurring international charges and minimize, to the extent possible, the different CSO contact numbers required to support non-domestic users.

-
9. Provide hot-links from the our public EIS website(s) to CSO functional area email addresses.
 10. Provide Telecommunications Device for the Deaf (TDD) access to the CSO for government representatives who are hearing impaired or have speech disabilities.
 11. Deal effectively with the geographical distribution of EIS subscribing agencies, GSA's Program Management Offices (PMOs) in the GSA regions, and GSA international activities.
 12. Provide responses to user inquiries of a general nature such as our established administrative and operational procedures, CTI points of contact, and user forum information.
 13. Provide information on available training classes as well as guidance and assistance with registration for training classes. Training requirements are described in G.10 Training.
 14. Provide technical support to agencies and the PMO regarding the services we deliver to the government. Technical support shall include, but not be limited to:
 - a) Answering questions related to how users can obtain the functions designed into the services we provide via the contract.
 - b) Advising users on the capabilities incorporated into service features.
 - c) Providing technical support to assist either our own or the agencies or other organization's technicians or personnel in the timely resolution of troubles.
 - d) Notifying users of new services and features that are planned or that have recently been added to the contract.
 - e) Providing ordering and tracking support services.
 - f) Providing support to help resolve billing issues.
 - g) Providing inventory management support.

2.6.2 Trouble Ticket Management (G.6.4)

CTI shall also shall provide, support and perform trouble ticket management in accordance with commercial best practices, and shall meet the government's requirements specified below.

2.6.2.1 Trouble Ticket Management General Requirements (G.6.4.1)

CTI shall create a trouble ticket for any reported and discovered service issues, provide status updates, provide online real-time access to trouble ticketing and system status information, update open trouble tickets and escalate as needed, and report the resolution to the initiator. The trouble ticket system used can be an existent or CTI provided system depending upon customer requirements.

CTI shall establish and implement procedures and systems for 24x7x365 trouble ticket and complaint collection, entry, tracking, analysis, priority classification, and escalation for all services to ensure that problems are resolved within the timeframes specified in Section G.8 Service Level Management.

As the first priority, CTI shall restore any TSP restoration coded service, as quickly as possible, using best effort.

CTI shall escalate issues according to the contractor's Program Management Plan (PMP) as described in the Program Management Plan.

2.6.2.2 Reporting Information (G.6.4.2)

CTI shall provide the government with the capability to query, sort, export, and save in formats such as PDF/CSV or standard/structured file formats trouble and complaint records by any field or combination of formatted (that is, not free-form text) fields in each record.

CTI shall process any credits applicable to the service outage based on this record of information. SLAs and credits are defined in Section G.8 Service Level Management.

CTI shall, upon request from the PMO and agencies, deliver archived trouble and complaint report data within five (5) days of the request for such information.

2.7 MINIMUM REQUIREMENTS FOR GEOGRAPHIC COVERAGE (C.1.3)

CTI will provide the EIS services on a global basis. CTI is offering 928 CBSAs, which is composed of all the CBSAs, excluding Alaska (), Hawaii (), and Puerto Rico (). This offering covers the minimum requirement as stated in C.1.3, of offering 25 of the top 100 CBSAs. CTI will provide the mandatory services, VPNS, ETS, IPVS, MNS, and AA, to all government locations within each of the 928 CBSAs offered.

2.8 SECTION 508 REQUIREMENTS (C.4)

2.8.1 Voluntary Product Accessibility Template (C.4.2)

As per the requirement in C.4.2, CTI will post the Voluntary Product Accessibility Template (VPAT) for each service identified in paragraphs C.4.4 below to our website, <http://www.coretechinc.com>, in order to demonstrate that our offerings comply with Section 508 standards.

2.8.2 Section 508 Applicability to Technical Requirements (C.4.3)

CTI understands that the EIS contract identifies the technical provision for services used by an agency to execute mission operations in Section C.2, Technical Requirements. CTI will ensure that services that execute mission operations will meet the relevant provision of Section 508, Subparts B, C, and D as identified in Section 4.4 or will provide the equivalent facilitation. CTI will reference Section G.5.3.1.3 for less than fully compliant products.

2.8.3 Section 508 Provisions Applicable to Reporting and Training (C.4.5)

CTI has reviewed Section G.9 Program Management, in order to understand the government's information reporting requirements. CTI will ensure that the required information will be reported via the Internet, email, or telephone. Any services that provide the required information will meet the relevant provisions of Section 508, Subparts B, C, and D or will provide equivalent facilitation.

Whenever training is required, it will be delivered via meeting and briefings, classroom, seminars, instructor-led and non-instructor on-line web based self-study, and manuals or desk top guides. For training delivered by the methods of meeting and briefings, classroom, and seminars, assistance such as signers and Braille products will be provided to disabled trainees when the government requests it in advance. For all training delivered by instructor-led and non-instructor on-line web based, the same capabilities provided for Internet reporting will be provided to disabled trainees.

3.0 RISK MANAGEMENT PLAN (G.9.4.10) [RIN: MTR0124-DN, MTR0147-DN, MTR0149-DN, MTR0150-DN, MTR0153-DN, MTR0154-DN]

CTI and its partners depend on information technology and the information systems to successfully carry out our business functions. Information systems and services that CTI will provide under the GSA EIS contract vehicle can include a range of diverse computing platforms from high-end supercomputers to personal digital assistants and cellular telephones. Information systems and services can also include very specialized systems and devices (e.g., telecommunications systems, industrial/process control systems, testing and calibration devices, command and control systems, and environmental control systems). Federal information and information systems are subject to serious threats that can have adverse impacts on organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation by compromising the confidentiality, integrity, or availability of information being processed, stored, or transmitted by those systems. Threats to information and information systems include environmental disruptions, human or machine errors, and purposeful attacks. Cyber-attacks on information systems today are often aggressive, disciplined, well-organized, well-funded, and in a growing number of documented cases, very sophisticated. Successful attacks on public and private sector information systems can result in serious or grave damage to the national and economic security interests of the United States. Given the significant and growing danger of these threats, it is imperative that CTI and our partners understand our responsibilities to federal agencies when they execute purchases under the EIS

solicitation and our requirements to have basic procedures in place for achieving adequate information security and for managing information system-related security risks.

The CTI Team has multiple risk mitigation strategies in place for the GSA EIS contract to provide basic security for all network services, as well as the network management systems and information systems and databases used to support those services. CTI's approach is a three tiered that addresses risk-related concerns at the organization level; the business process level and the information systems or network level. Since communications services under this contract will carry non-sensitive programmatic and administrative traffic, Controlled Unclassified Information (CUI) traffic, and higher levels of sensitive and/or classified traffic up to and including Top Secret/SCI that may be encrypted by agency users CTI realizes that the risk mitigation plan applies not only to services provided, but the facilities that house the services, the physical location security plan, the products and services delivered to our physical locations and the data that is transported over the various networks and the databases residing at CTI. Starting with information systems first, CTI follows the basic risk management framework process below in addressing the formulation of a risk management plan for federal information systems.

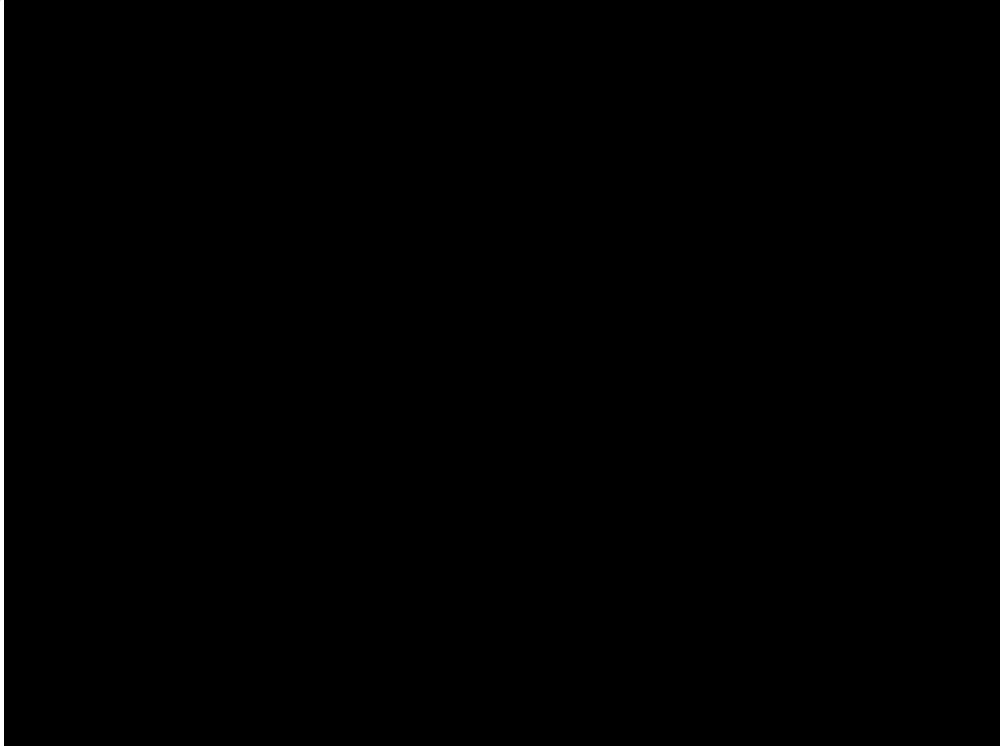


Figure 21: Risk Management Framework Process

The schematic is broken into five phases or tasks for Federal information and information systems in putting together CTI's risk mitigation strategy. [REDACTED]

[REDACTED]

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

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

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]

[Redacted text block]

- [Redacted list item]
- [Redacted text block]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

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

[Redacted text block containing multiple paragraphs of information, all obscured by black bars.]

CTI provide s basic security for all network services, as well as the network management systems and information systems and databases used to support those services. Such security includes protecting all network services, information, CTI infrastructure, and information processing resources against threats, attacks, or failures of systems. Our risk mitigation plans are comprised of both formal and expert based mitigation. [REDACTED]

[REDACTED]

[REDACTED] As part of our overall approach the CTI risk management strategy is propagated within our organization and to business partners and contractors, some of whom may have programmatic, planning, developmental, acquisition, operational, and oversight responsibilities.

Our other forma programs start with the knowledge that regulations, procedures and processes are continually developed, reviewed, assessed and updated by the government and have been for decades based on industry and government standards, technical innovation, and market trends. These policies are generally technically superior to Ad Hoc policies or agreements developed by commercial entities that may be market driven as opposed to being based on national security requirements, and only suggest or recommend risk mitigation strategies as opposed to governmental policies that demand compliance and standardization.

CTI shall follow all government policies, rules and regulations that mitigate risk for clients and the CTI team in delivering services to government clients. Additionally, CTI and its partners shall develop and keep current all policy and procedures documents, as outlined in the specified NIST documents as well as appropriate GSA IT Security Procedural Guides that cover all network services, information, contractor infrastructure, and information processing resources against threats, attacks, or failures of systems. The following documents shall be verified and reviewed during the initial security and

risk mitigation assessment and updates provided to the GSA COR/ISSO/ISSM

biennially:

- a) Access Control Policy and Procedures (NIST SP 800-53 R4: AC-1).
- b) Security Awareness and Training Policy and Procedures (NIST SP 800-53 R4: AT-1).
- c) Audit and Accountability Policy and Procedures (NIST SP 800-53 R4: AU-1).
- d) Security Assessment and Authorization Policies and Procedures (NIST SP 800-53 R4: CA-1).
- e) Configuration and Management Policy and Procedures (NIST SP 800-53 R4: CM-1).
- f) Contingency Planning Policy and Procedures (NIST SP 800-53 R4: CP-1).
- g) Identification and Authentication Policy and Procedures (NIST SP 800-53 R4: IA-1).
- h) Incident Response Policy and Procedures (NIST SP 800-53 R4: IR-1).
- i) System Maintenance Policy and Procedures (NIST SP 800-53 R4: MA-1).
- j) Media Protection Policy and Procedures (NIST SP 800-53 R4: MP-1).
- k) Physical and Environmental Policy and Procedures (NIST SP 800-53 R4: PE-1).
- l) Security Planning Policy and Procedures (NIST SP 800-53 R4: PL-1).
- m) Personnel Security Policy and Procedures (NIST SP 800-53 R4: PS-1).
- n) Risk Assessment Policy and Procedures (NISTSP 800-53 R4: RA-1).
- o) Systems and Services Acquisition Policy and Procedures (NIST SP 800-53 R4: SA-1).
- p) System and Communication Protection Policy and Procedures (NIST SP 800-53 R4: SC-1).
- q) System and Information Integrity Policy and Procedures (NIST SP 800-53 R4: SI-1).

- r) NIST Special Publication, 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach
- s) All Federal Information Security Management Act (FISMA), DOD, and Intelligence Community requirements where applicable

From a corporate perspective, at the organizational level, CTI considers, as part of an overall risk mitigation plan, all security threats both internal and external. Employees could be internal threats simply by their sheer ability to gain access to corporate spaces and other areas where they may have approved access and can use their knowledge of the company, policies and procedures to wreak havoc by stealing or destroying critical equipment and/or accessing critical information technology systems, . Fire, water, and environmental failures are also internal threats.

[REDACTED]

At the business level CTI activities are closely associated with our business model and business support system (BSS) which is aligned with our enterprise architecture and our

business processes for CTI, which covers both commercial and government activities (including any derivative or related missions and business processes carried out by our partners and/or sub-contractors). As CTI deals with both commercial and government entities CTI follows NIST 800-37 Rev 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach," on a modified basis compatible with our business practices. CTI's corporate wide information protection strategy is continually updated to incorporate ever-changing information security requirements. [REDACTED]

[REDACTED]

CTI's commitment to security in general extends to servicing any TO recieved on the GSA EIS vehicle 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 with a TO.

[REDACTED]

[REDACTED]

CTI's contracts have covered a wide array of telecommunication services, some geared toward 8a certified companies and small businesses through Indefinite Delivery, Indefinite Quantity (IDIQ), multiple-award, fixed price, performance-based contract with an Economic Price Adjustment. Our GSA contracts have covered a wide range of services to include Cable Installations, Voice, Data, Video, Converged Services, Integrated IT Solutions allowing for seamless connectivity for agency voice, data, and video; and other Wired Telecommunication services within multiple NAICS codes. Additionally, our business experience had provided GSA and their Federal customers with decades of service proven products services such as:

- Physical Security
- Network Security/Information Systems Security
- Personnel Security
- Warehousing
- Finished Goods Inventory
- Defective Inventory
- Disposal
- Parts Procurement/Management
- Warranty Management
- Advance Exchange
- Go/No-Go Testing
- Reverse Logistics Pipeline Management
- Parts
- Deployment/fulfillment
- Asset Recovery
- Re-Deployment

For business risk mitigation strategies, the CTI Team employs industry standard risk mitigation strategies that mimic the standards template approach used in NIST 800-30, NIST 800-30, and NIST 800-37 Rev 1 “Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach,” are consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b (3), Securing Agency Information Systems, as analyzed in Circular A-130, Appendix IV: Analysis of Key Sections, Supplemental information is provided in Circular A-130, Appendix III, Security of Federal Automated Information Resources and the risk application we use is compliant with IEEE 1012, 1540 and ISO 16085 and 31000.

[Redacted content]

[REDACTED]

[REDACTED]

Our Human Resource Management team ensures we employ only the most highly skilled and trustworthy personnel who have customer service and satisfaction at the forefront of their corporate goals and have passed background checks based on corporate access needs.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The ultimate benefit of these tools are not only to effectively and efficiently perform risk planning, but also to communicate and level-set the corporate executives, middle management and the entire CTI Team staff on risk issues and their handling within the CTI Team. At CTI, we have internal training classes that teach our personnel how to develop risk information to enter into a risk plan and strategies to improve our customer and contractual response obligations. Skills in our risk training that we include are:

- Defining program, contractual and customer oriented risk.
- Describing characteristics of risks.
- Describing benefits of using risk management techniques across the CTI Team enterprise.
- Describing the role of personnel who can mitigate risk and enforce or improve risk management strategies.
- Describing and showcasing the risk management process within the CTI Team enterprise.
- Describe how the CTI Team uses group techniques to identify contractual and customer focused risks, and Program management risks.
- Analyze and Classify risks.

- Evaluate/prioritize risks.
- Develop risk mitigation strategies.
- Describe risk tracking/monitoring methods used to document and update risk and program plans.

Much of the risk mitigation is geared toward contract, program management and cyber security issues. Within the cyber-security category risk evaluation and mitigation is contained with the CTI Team SCRM Plan and within the Business Support System Framework.

[REDACTED]

In order to ensure our [REDACTED] system is adequate to meet the requirements of the GSA EIS contract vehicle, the BSS Verification Test Plan and Development and Implementation Plan is critical to ensure that the BSS can support the customer base as envisioned within the GSA EIS RFP. This test plan is submitted under a separate enclosure within the solicitation response.

[REDACTED]

[REDACTED]

Our CTI Team BSS application provides the team an all-in-one solution that is scalable and highly available, platform independent, open and extensible. The system provides features that match the needs of the GSA EIS vehicle. [REDACTED]

[REDACTED]

[REDACTED]

In addition to complying with the requirements identified in government policies, directives and guides, the CTI Team will comply with current GSA policies, directives and guides listed within the GSA EIS RFP.

The CTI Team's BSS system also uses and/or can use the following software systems to provide the Managed Security Services (MSS) which are part of the BSS. [REDACTED]

[REDACTED]

3.1 CTI RISK MANAGEMENT PLAN FOR IDIQ AND TASK ORDERS

3.1.1 IDIQ Level Risk Management Plan and TO Risk Management Plan (NIST 800-37 R1)

The CTI Team's approach to any IDIQ level risk management approach is to [REDACTED]

[REDACTED]

[REDACTED]

The Risk management approach combines several factors [REDACTED]

[REDACTED]

[REDACTED]. All plans and processes combined are geared to risks across the enterprise from strategic to tactical as described in NIST publication 800-39 as show below:

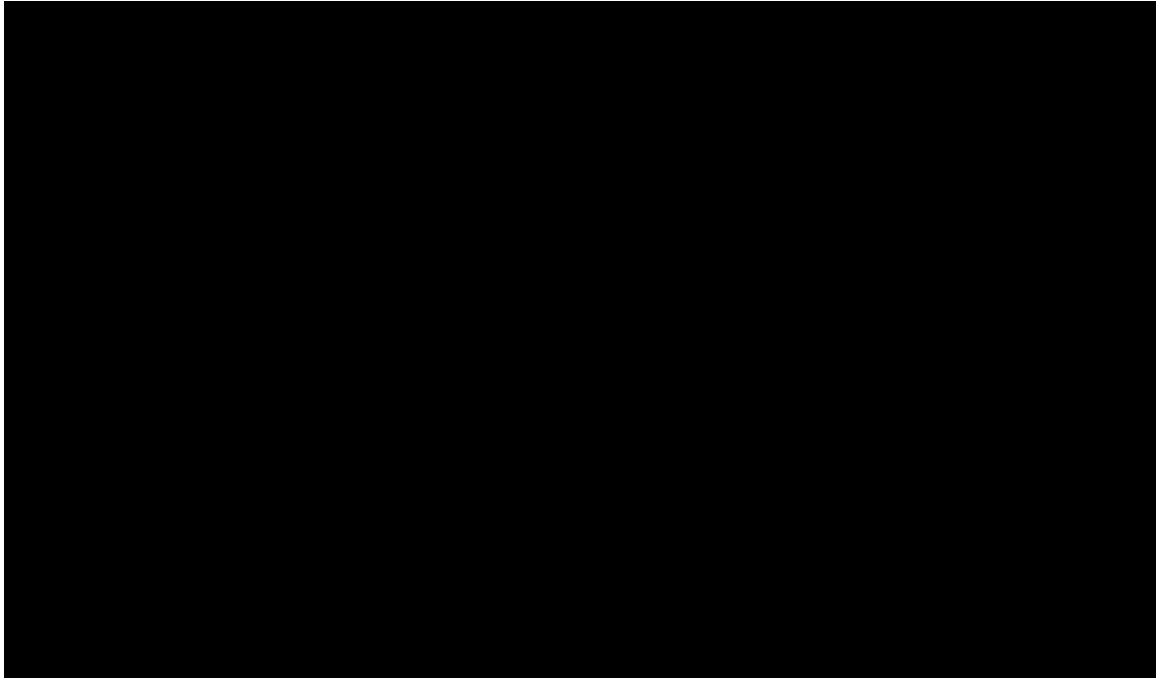
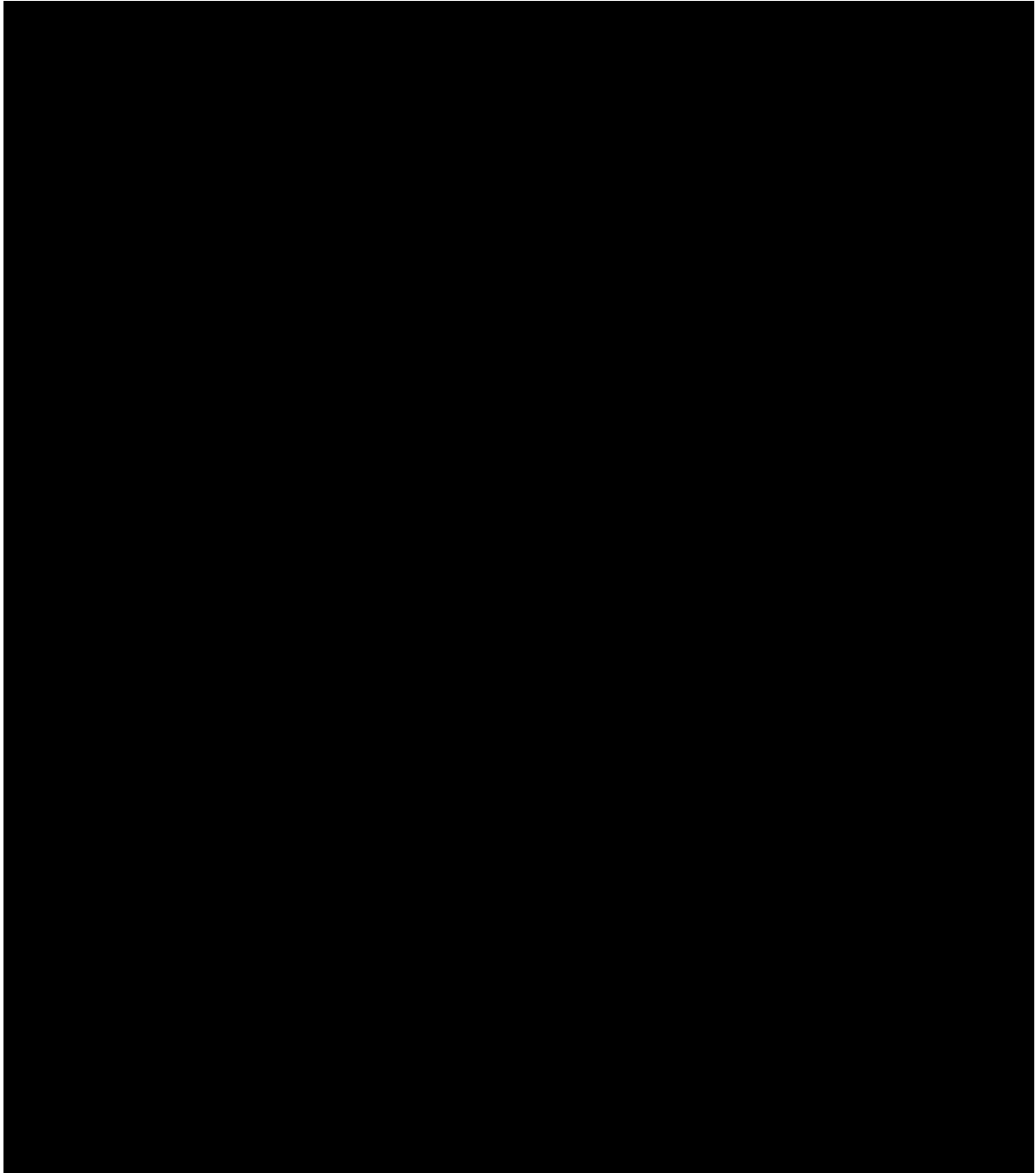
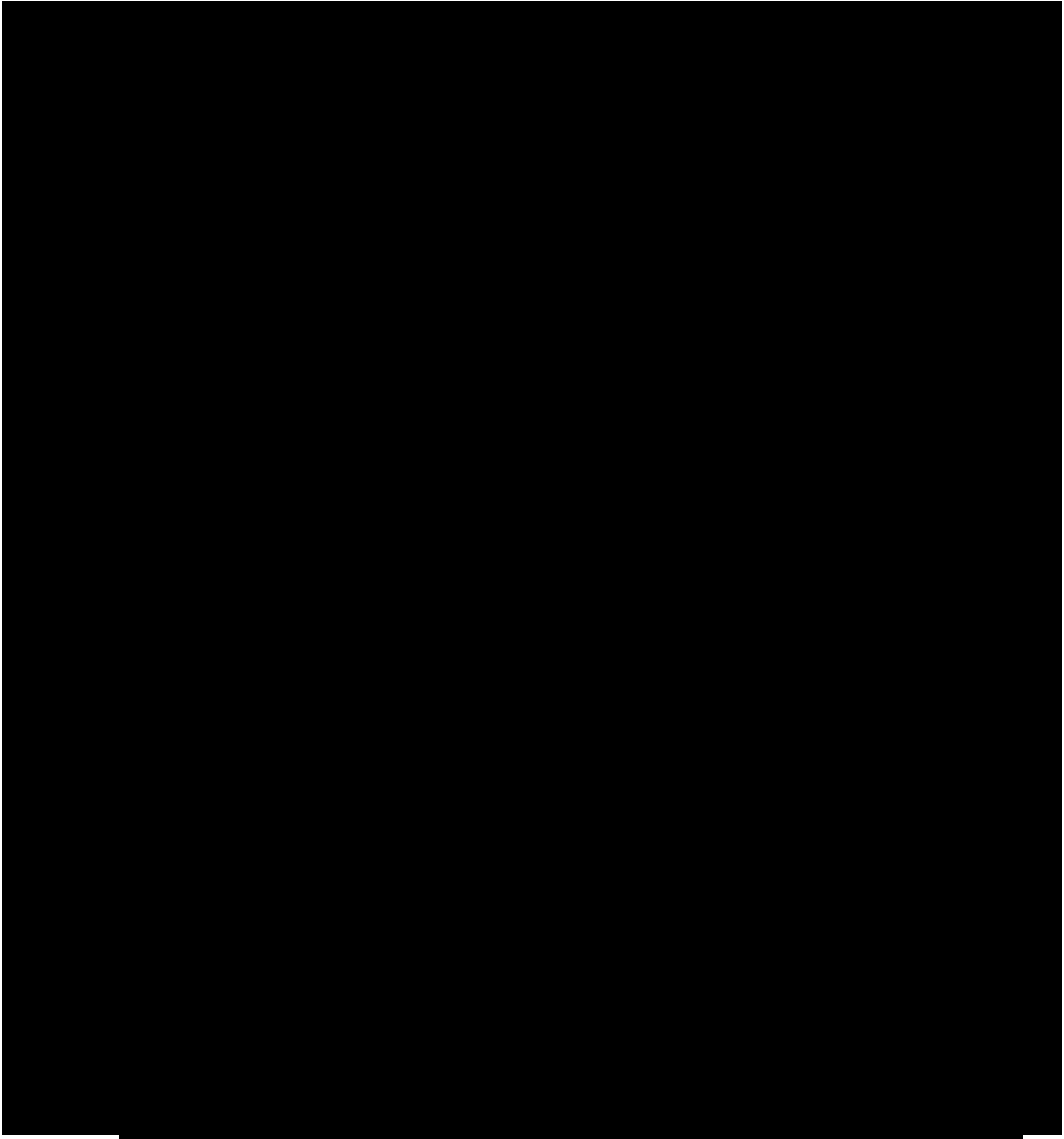


Figure 22: The SCRM Plan Tiers – CTI's approach to Risk-Based decisions based on traceability, transparency, accountability and continuous improvement.

The constructs of the combined systems and processes can be summed up to key tasks which are contained at every level of the CTI Team enterprise. [REDACTED]

[REDACTED]



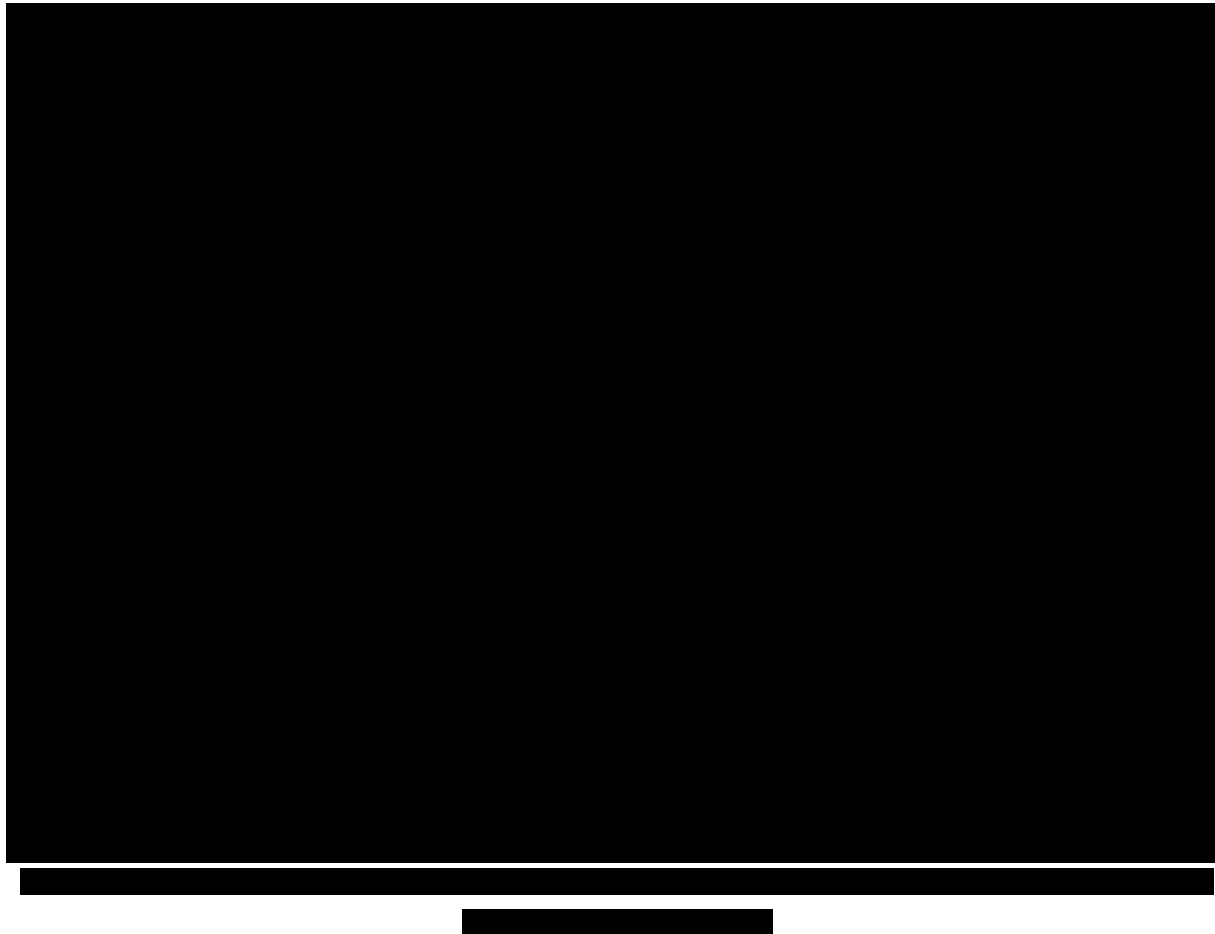


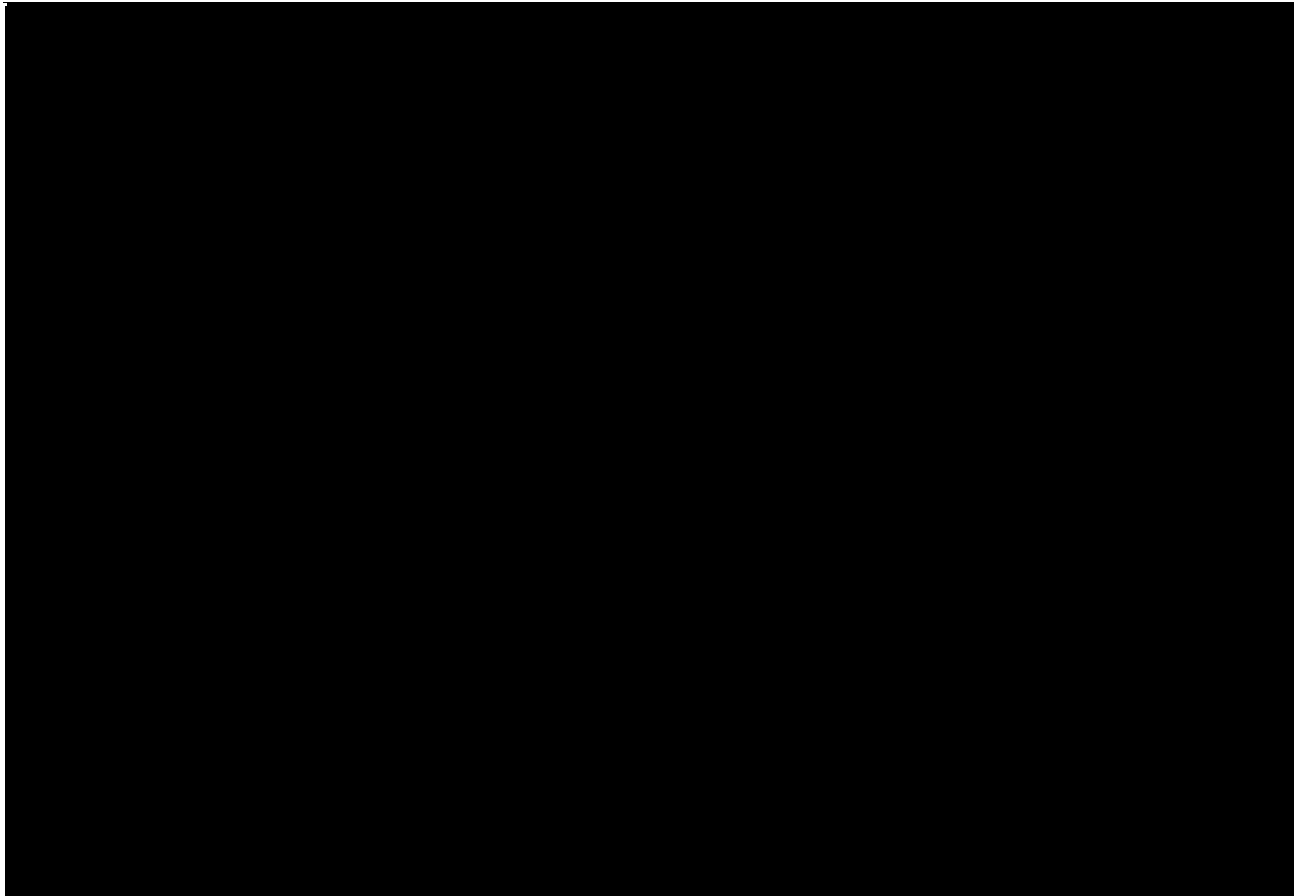
[REDACTED]

The type of data that results from the NIST process charts illustrated above are incorporated into [REDACTED], thus the Approach, categorization of the Risk, Selection of appropriate risk strategies, Implementation of Solutions, Assessment of solutions/outcomes, Authorizations,

Monitoring and Status and Reporting are all part of the process of filling out the Risk Assessment for each project that requires a full-fledged Risk Assessment, whether for the GSA EIS IDIQ as a whole, or for performing on an Task Orders under the IDIQ, or for corporate risk assessment pertaining to the risks associated with bidding on a Task Order. [REDACTED]

All of the subcomponent steps described above and contained in the reference materials such as NIST 800-39 have been incorporated into our [REDACTED] software which can be seen in the screen shots below:





[REDACTED]

Risk levels are set by CTI's personnel at the appropriate level of their authority. Within the CTI Team, from a corporate perspective we also look at opportunity risks which can apply to Task Orders in terms of risk of acceptance or bid. The assumption may be that all task orders are good from a corporate perspective when in fact, accepting or bidding on certain task orders may be detrimental to the financial well-being of a company. [REDACTED]

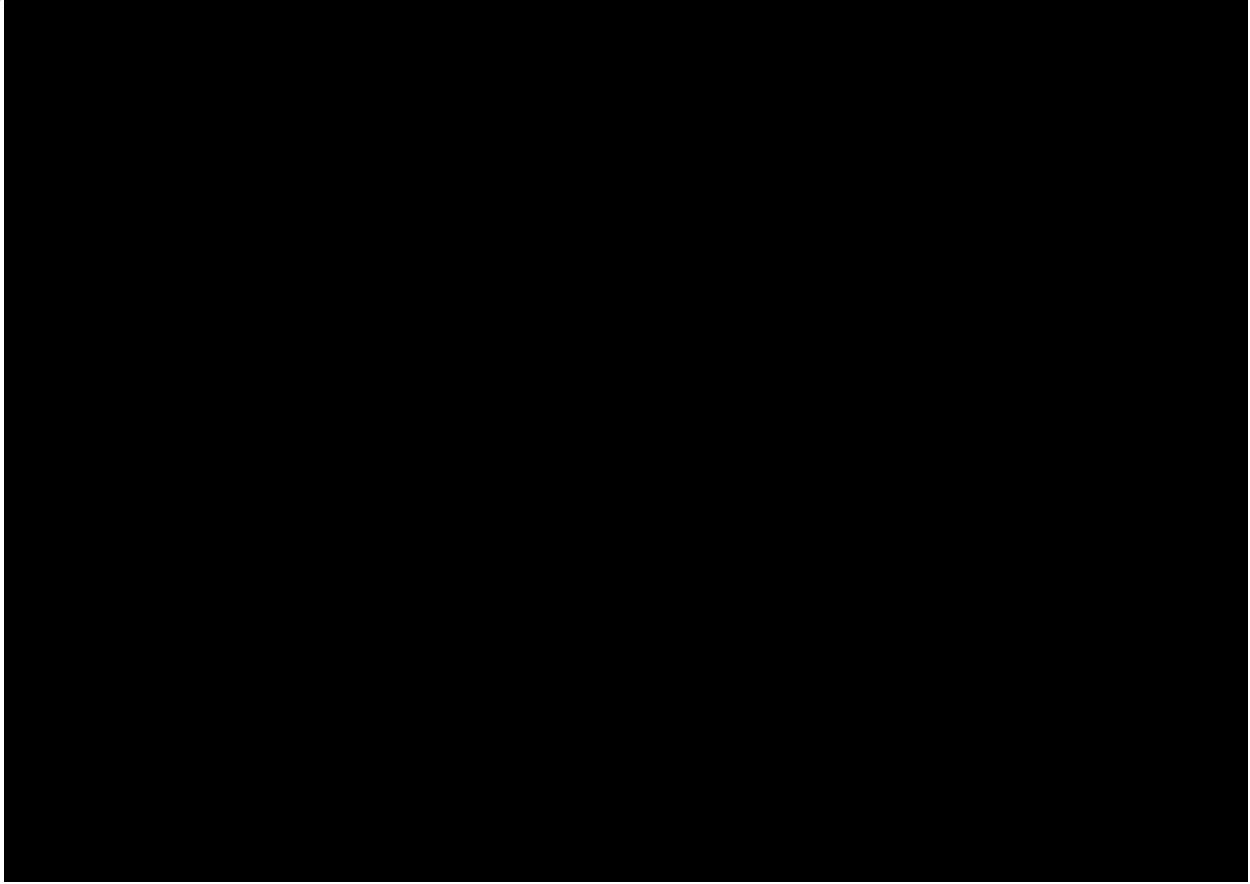
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

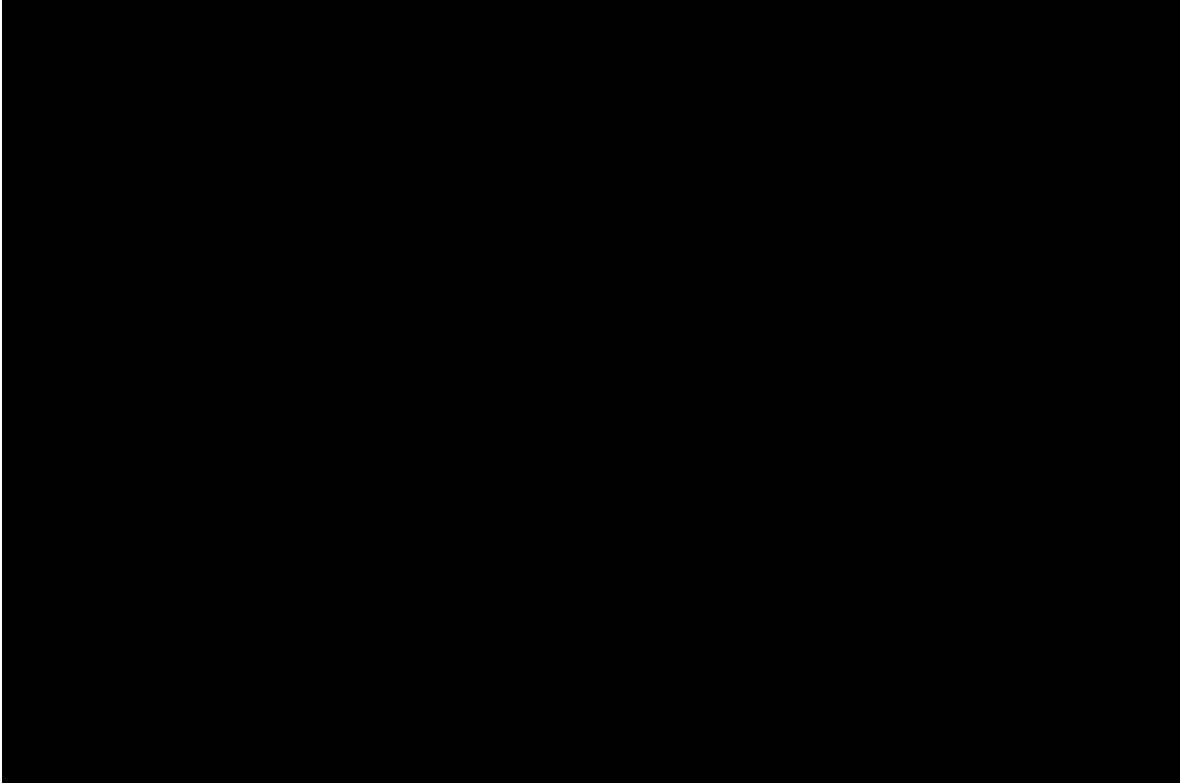


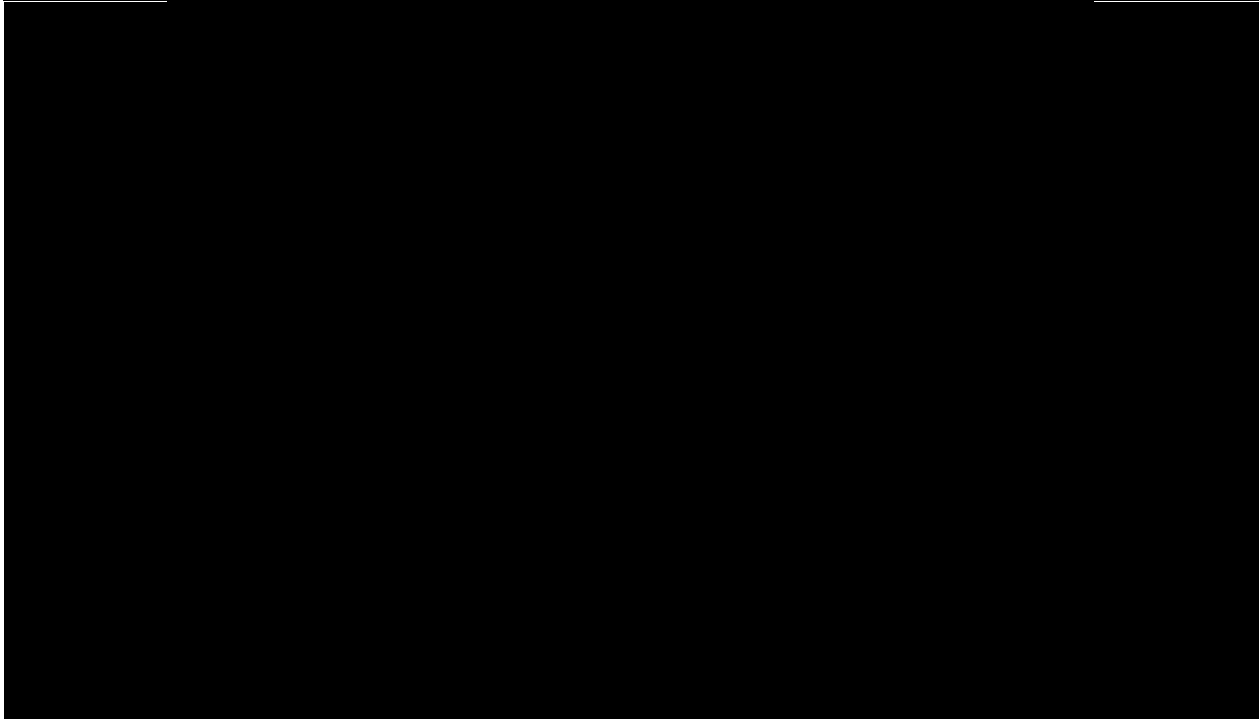


I

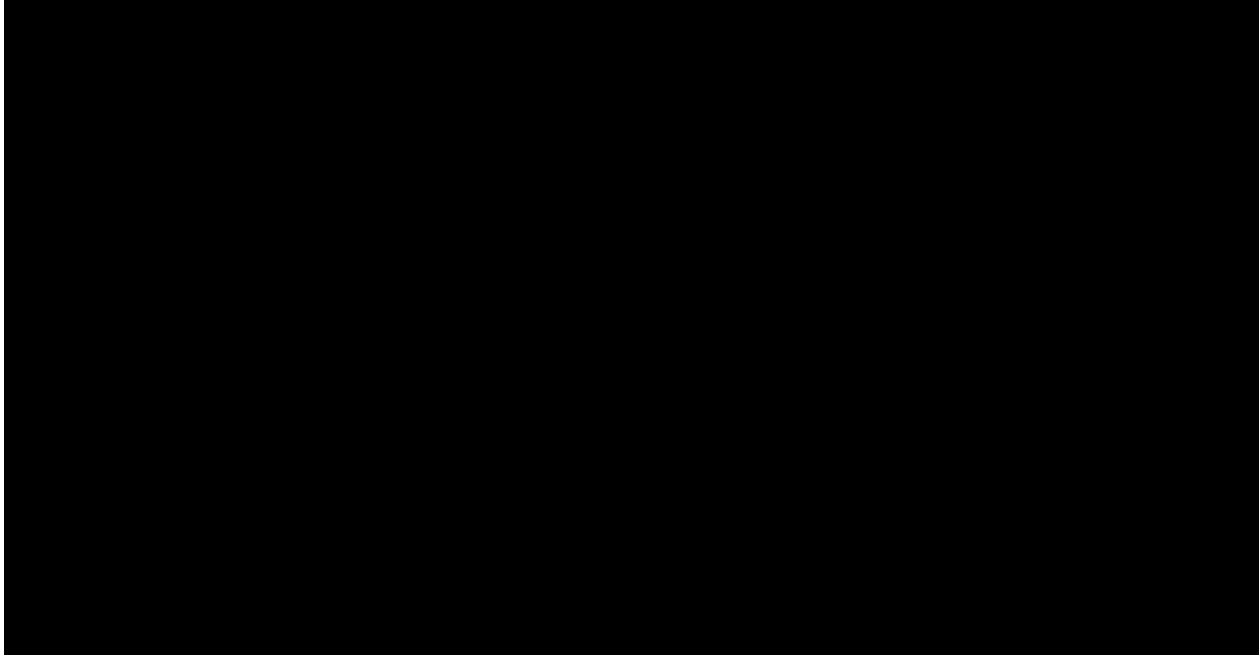
3.1.1.1 Risk triggers

Risk triggers allow the CTI Team to set tripwires that key personnel whenever a specified risk approaches a set point or tripwire that requires specific actions to be taken and specific personnel to be notified. User permission ensures data is protected at every level of risk.

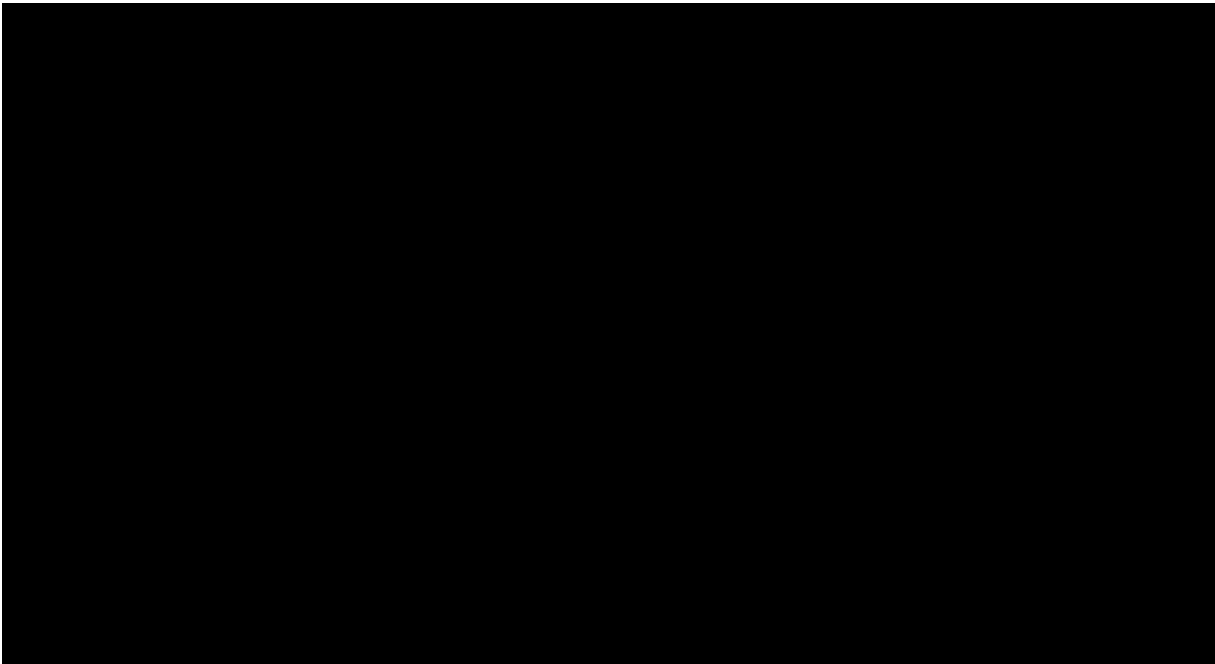


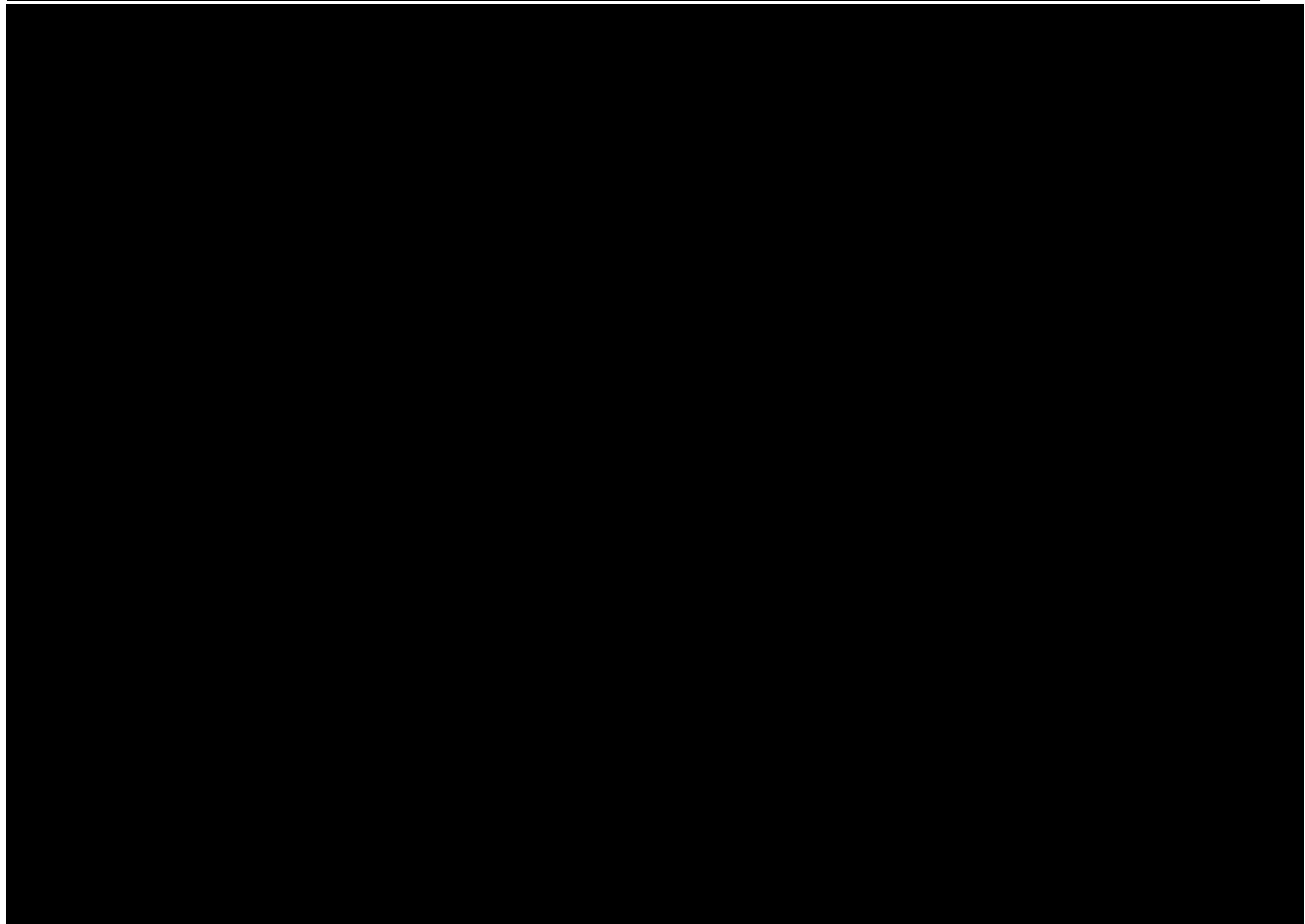


The CTI Team can inject specific parameters for each risk using the Risk Details screen and Risk Mitigation (next page) allows us to input mitigation characteristics for each risk type..



Mitigation Steps





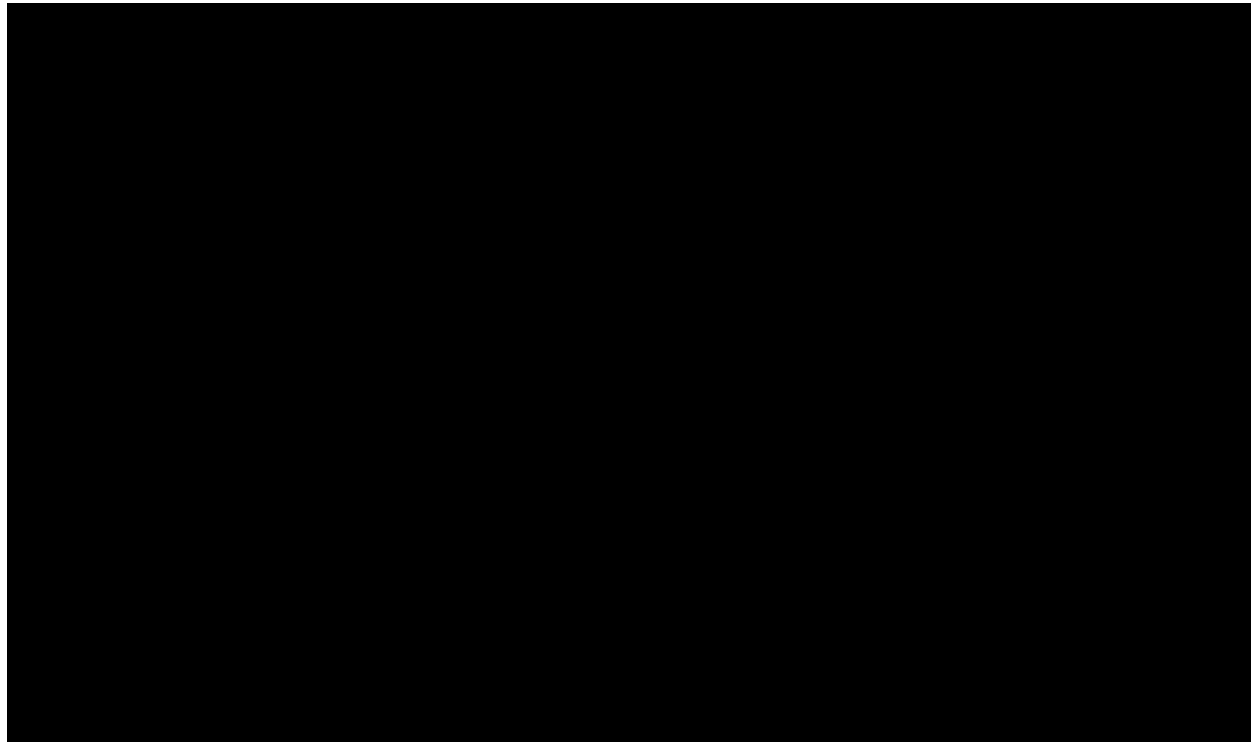
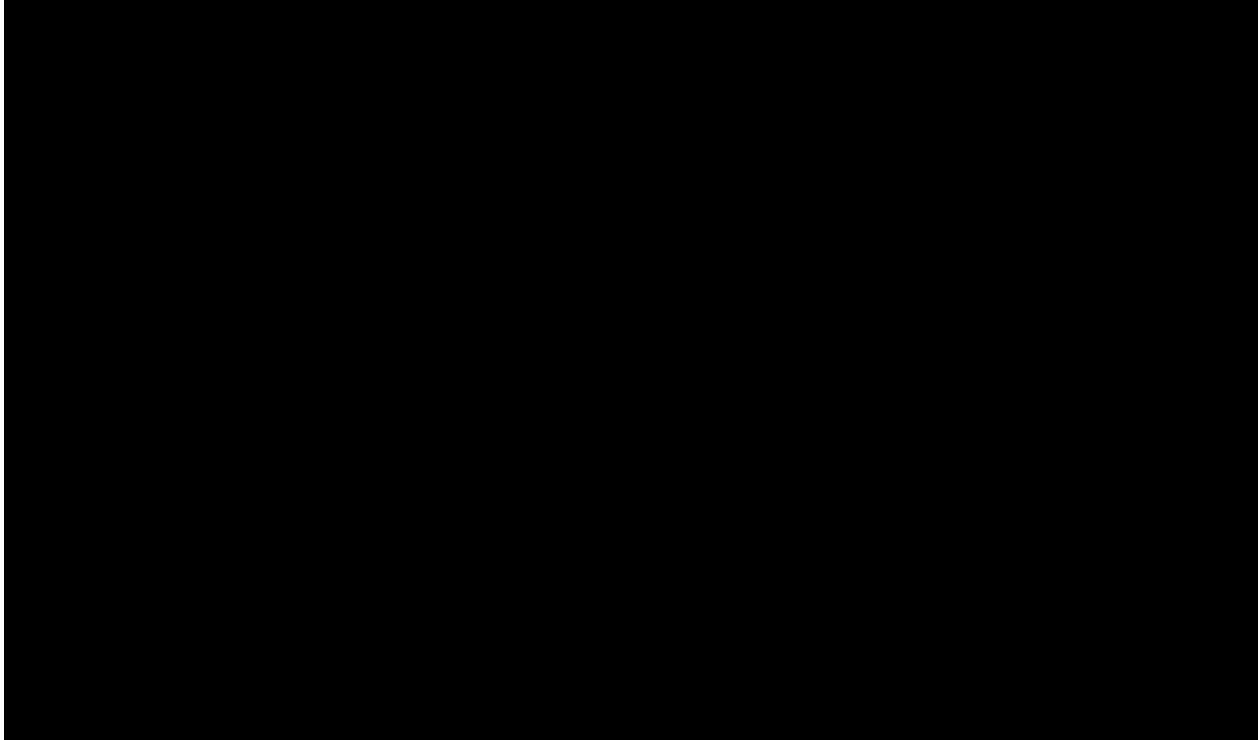
The Association screen allows CTI Team members to associate certain risks to another risk, which could be in another project/program or impact a supplier associated risk. [REDACTED]

[REDACTED]

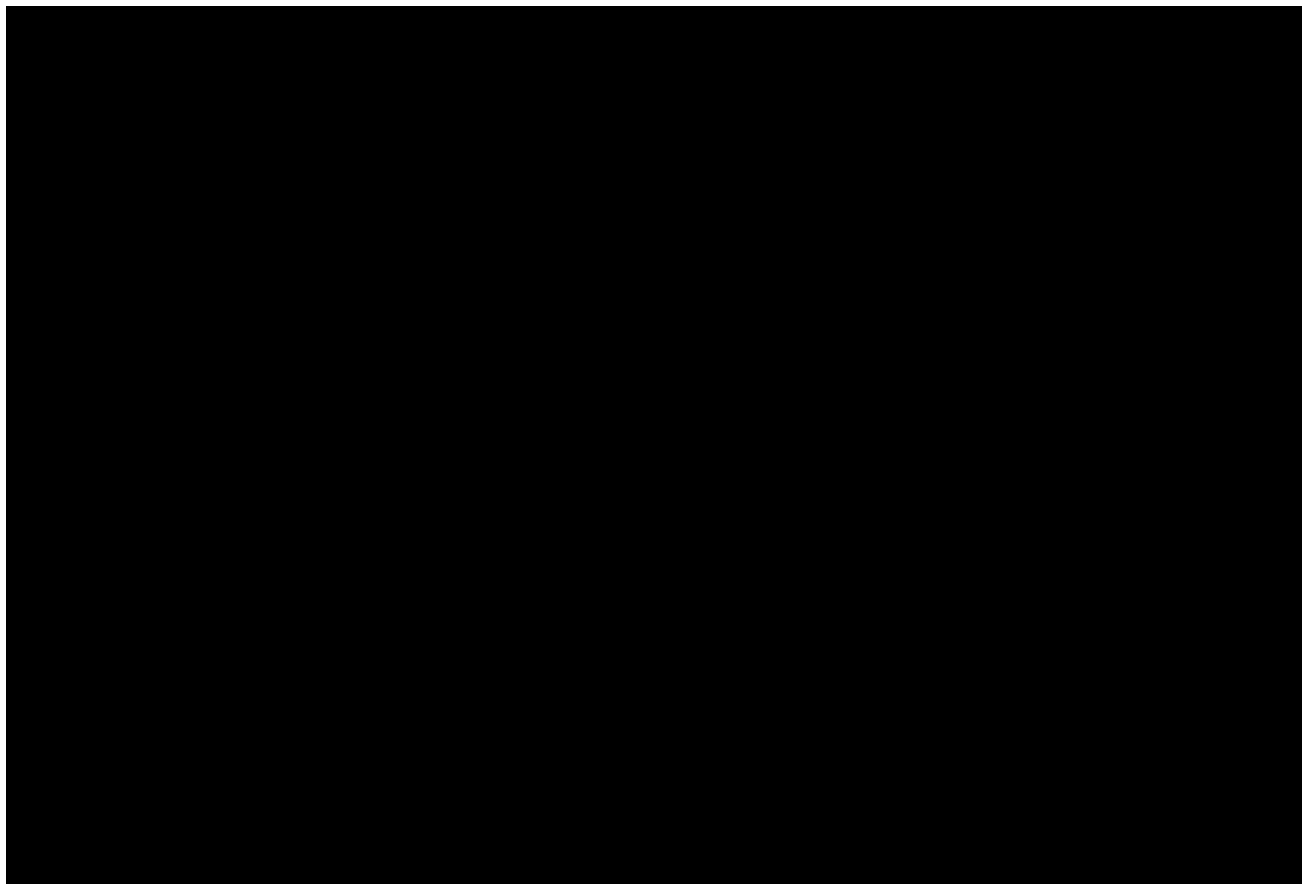
[REDACTED]

[REDACTED]

[REDACTED]



The prioritization and Risk State screens show the risk exposure and risk impact dates and change as the environment or status of risk parameters change. Finally there are a variety of Risk Reports which can be provided internally and/or shared with clients as required to allow affected personnel to remain aware of risk so everyone in the chain can be made fully aware of the dynamic nature of Risk Management. Thus all involved can become informed whenever events – either controllable or uncontrollable impact the IDIQ, delivery/budget schedules and/or mission status of the Federal agency customer.



4.0 SUBMISSION MATRIX (L.29.2.4)

Requirement ID	Matrix Volume	RFP Reference(s)	Description	Service Name	Area Name	Service ID	File Volume	File Provided (Y/N)	File Name	Proposal Section	Page Number