



General Services Administration (GSA)
Federal Acquisition Service (FAS)
Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

"Enabling Agency Missions through Innovative,
Integrated, and Secured Solutions"

GS00Q17NSD3000, September, 2022

Volume 1 – Technical





General Services Administration (GSA)
Federal Acquisition Service (FAS)
Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

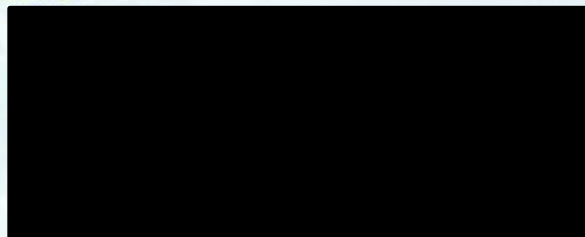
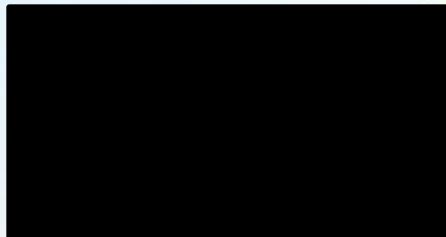
"Enabling Agency Missions through Innovative,
Integrated, and Secured Solutions"

GS00Q17NSD3000
Volume 1 — Technical
September, 2022

Submitted via AcquiServe™ Portal:
Timothy Horan, FAS EIS Contracting Officer
1800 F St NW
Washington, DC 20405

Submitted by:

AT&T Corp.
3033 Chain Bridge Road
Oakton, VA 22124



RESTRICTION ON DISCLOSURE AND USE OF DATA

This proposal or quotation includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed – in whole or in part – for any purpose other than to evaluate this proposal or quotation. If, however, a contract is awarded to this offeror or quoter as a result of – or in connection with – the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction is contained in all pages that carry the legend of "Use or disclosure of the data on this page is subject to the restrictions on the title page of this proposal document."

AT&T - PROPRIETARY

This document contains confidential, trade secret, commercial or financial information owned by AT&T Corp. and is voluntarily submitted for evaluation purposes only. It is exempt from disclosure under the Freedom of Information Act (5 U.S.C. 552) under Exemption (b) (4), and its disclosure is prohibited under the Trade Secrets Act (18 U.S.C. 1905).

CONTRACTOR BID OR PROPOSAL INFORMATION

This bid or proposal shall not be disclosed to evaluators outside the Government, except pursuant to a nondisclosure agreement between the evaluator and AT&T.



TABLE OF CONTENTS

VOLUME 1 — [L.29; L.11; M.2.1; C.1; C.2; C.4]	1
1 Proposed Network Architecture [L.29(1); L.29.1; M.2.1]	1
1.1 Understanding [L.29.1(A); M.2.1(1); C.1]	4
1.1.1 [REDACTED]	12
1.1.2 Interoperability [C.1.8.6]	13
1.1.3 National Security Emergency Preparedness (NS/EP) [C.1.8.8]	13
1.1.4 IPv6 [C.1.8.8]	14
1.1.5 Network Function Virtualization/Software-Defined Networking [C.1.6]	15
1.1.5.1 Software Defined Network (SDN) [C.1.6]	16
1.1.5.2 Network Function Virtualization (NFV) [C.1.6]	17
1.1.5.3 NFV/SDN Benefits [C.1.6]	18
1.1.5.4 NFV/SDN Security and Standard [C.1.6]	18
1.2 Quality of Services [L.29.1(B); M.2.1(2)]	19
1.2.1 Compliance [M.2.1(2)]	19
1.2.2 Scalability [M.2.1(2)]	19
1.2.3 Reliability [M.2.1(2)]	20
1.2.4 Resilience [M.2.1(2)]	20
1.2.5 Event Management Framework	23
1.2.6 Network Disaster Recovery	24
1.3 [REDACTED]	25
1.4 [REDACTED]	32
1.4.1 [REDACTED]	32
1.4.2 [REDACTED]	33
1.4.3 External Traffic Routing Requirements [L.29.2.3; M.2.1(4)(c); C.1.8.8]	33
1.4.3.1 Methodology for Identifying AT&T's Participating Agency Traffic for Each Affected Service [L.29.2.3(1); M.2.1(4)(c)(i)]	35
1.4.3.2 [REDACTED]	35
1.4.3.3 [REDACTED]	36

1.4.3.4	[REDACTED]	36
1.4.3.5	[REDACTED]	36
1.4.3.6	[REDACTED]	37
1.4.3.7	Availability of TS/SCI Cleared Personnel for “Smart-Hands” Service of DHS Supplied Equipment [L.29.2.3(7); M.2.1(4)(c)(vii)]	37
1.4.3.8	Instrumentation to Measure Transport of SLA KPIs [L.29.2.3(8); M.2.1(4)(c)(viii); C.1.8.8]	37
1.4.4	Traffic Identification and Routing Policy [L.29(2)(c); L.29.2.3; C.1.8.8(3)]	38
1.4.4.1	[REDACTED]	38
1.4.4.2	[REDACTED]	38
1.4.4.3	[REDACTED]	38
1.4.4.4	Operation of AT&T Aggregation Service [L.29.2.3]	38
2	Technical Response [L.29(2); L.29.2; M.2.1; C.1; C.2]	39
2.1	Mandatory EIS Services [L.29(2)(a); L.29.2.1; M.2.1; C.1.2]	39
2.1.1	Service Area: Data Service [C.2.1]	39
2.1.1.1	Virtual Private Network Service [L.29.2.1; M.2.1; C.2.1.1]	39
2.1.1.2	Ethernet Transport Service [L.29.2.1; M.2.1; C.2.1.2]	49
2.1.2	Service Area: Voice Service [L.29.2.1; M.2.1; C.2.2]	56
2.1.2.1	[REDACTED]	57
2.1.2.2	Circuit Switched Voice Service [L.29.2.1; M.2.1; C.2.2.2]	69
2.1.3	Service Area: Managed Service [C.2.8]	77
2.1.3.1	Managed Network Service [L.29.2.1; M.2.1; C.2.8.1]	77
2.1.4	Service Area: Access Arrangements [C.1.8.1]	87
2.1.4.1	Access Arrangements [L.29.2.1; M.2.1; C.2.9]	87
2.1.5	Section 508 Requirements [C.4]	95
2.1.5.1	Background [C.4.1]	95
2.1.5.2	Voluntary Product Accessibility Template [C.4.2]	96
2.1.5.3	Section 508 Applicability to Technical Requirements [C.4.3; C.2]	97
2.1.5.4	Section 508 Provisions Applicable to Technical Requirements [C.4.4]	97
2.1.5.5	Section 508 Provisions Applicable to Reporting and Training [C.4.5]	97

2.2		98
2.2.1		98
2.2.1.1		98
2.2.1.2		106
2.2.1.3		112
2.2.1.4		118
2.2.1.5		124
2.2.1.6		131
2.2.2		137
2.2.2.1		137
2.2.2.2		146
2.2.3		152
2.2.3.1		152
2.2.4		162
2.2.4.1		162
2.2.5		168
2.2.5.1		171
2.2.5.2		177
2.2.5.3		182
2.2.5.4		187
2.2.6		193
2.2.6.1		193
2.2.7		199
2.2.7.1		200
2.2.7.2		206
2.2.8		210
2.2.8.1		210
2.2.8.2		216
2.2.8.3		222
2.2.8.4		234
2.2.8.5		250
2.2.8.6		261
2.2.8.7		268
2.2.8.8		274

2.2.8.9	[REDACTED]	283
2.2.9	[REDACTED]	291
2.2.9.1	[REDACTED]	291
2.2.10	[REDACTED]	293
2.2.10.1	[REDACTED]	293
2.2.11	[REDACTED]	293
2.2.11.1	[REDACTED]	293
2.3	Traffic Identification and Routing Policy [L.29(2)(c); L.29.2.3; M.2.1(4)(c);C.1.8.8(3)]	295
2.3.1	Detailed Technical Description [L.29.2.3; C.1.8.8]	295
2.3.2	Technical Viability of AT&T's Aggregation Service [L.29.2.3(1)- L.2.9.2.3(8)]	295
Appendix A — Risk Management Framework Plan [L.29(3)(a); L.29.2.2; L.11; C.1.8.7; C.1.8.7.4]		
	Ensurance of Delivery of System Security for the EIS Services [L.29.2.2; C.1.8.7; C.1.8.7.4]	A-1
A-1	The AT&T Risk Management Framework Plan [C.1.8.7; C.1.8.7.4]	A-2
A-2	The AT&T RMF Plan Management and Oversight [C.1.8.7]	A-8
A-2.1	IA Organization Team Alignment in Support of the RMF Plan [C.1.8.7]	A-9
A-2.2	IA Organization Team Alignment in Support of the RMF Plan [C.1.8.7; C.1.8.7.7]	A-9
A-2.3	Implementation of Security Controls [C.1.8.7]	A-20
A-2.4	Assessment of Security Control Effectiveness [C.1.8.7]	A-21
A-2.5	Authorization of the Information System [C.1.8.7]	A-21
A-2.6	Ongoing Monitoring of Security Controls and the Security State of the Information System [C.1.8.7]	A-24
Appendix B — MTIPS Risk Management Framework Plan [L.29(3)(b); L.29.2.2; L.11; C.1.8.7; C.1.8.7.1; C.2.8.4.5; C.2.8.4.5.5]		
	Ensurance of Delivery of System Security for MTIPS [L.29.2.2; C.1.8.7; C.2.8.4.5]	B-1
B-1	The AT&T MTIPS Risk Management Framework Plan [C.2.8.4.5.2; C.2.8.4.5.5]	B-2
B-2	The AT&T MTIPS RMF Plan Management and Oversight [C.2.8.4.5; C.2.8.4.5.2]	B-7
B-2.1	IA Organization Team Alignment in Support of the MTIPS RMF Plan [C.2.8.4.5.2]	B-9
B-2.2	IA Organization Team Alignment in Support of the RMF Plan [C.2.8.4.5.4; C.2.8.4.5.5; C.2.8.4.5.5.1]	B-9



B-2.3	Implementation of Security Controls [C.2.8.4.5.2].....	B-20
B-2.4	Assessment of Security Control Effectiveness [C.2.8.4.5.2]	B-21
B-2.5	Authorization of the Information System [C.2.8.4.5.3; C.2.8.4.5.4(19-21, 24-27)]	B-21
B-2.6	Ongoing Monitoring of Security Controls and the Security State of the Information System [C.2.8.4.5.4; C.2.8.4.5.5]	B-26
Appendix C — Assumptions and Conditions [L.9]		C-1
C-1	Assumptions and Conditions [L.9]	C-1



LIST OF FIGURES

Figure 1.1-1. T	9
Figure 1.1.4-1.	14
Figure 1.1.5-1. Software Defined Network Architecture.	16
Figure 1.1.5-2. Virtualization of Customer Premises and PE.	17
Figure 1.1.5-3. Service Model for an SDN with NFV	18
Figure 1.2.5-1. Event Management Framework.	23
Figure 1.2.6-1.	24
Figure 1.2.6-2.	25
Figure 1.4.3-1.	33
Figure 2.1.1-1.	41
Figure 2.1.1-2.	45
Figure 2.1.1-3.	50
Figure 2.1.2-1.	59
Figure 2.1.2-2.	66
Figure 2.1.2.2-1.	70
Figure 2.1.3-1.	80
Figure 2.1.3-2.	81
Figure 2.1.4-1.	90
Figure 2.1.5-1. AT&T Section 508 Compliance Implementation Methodology.	96
Figure 2.2.1-1.	99
Figure 2.2.1-2.	107
Figure 2.2.1-3.	112
Figure 2.2.1-4.	119
Figure 2.2.1-5.	125
Figure 2.2.1.6-1.	132
Figure 2.2.2-1.	138
Figure 2.2.2.2-1.	147
Figure 2.2.3-1.	152
Figure 2.2.4-1.	163
Figure 2.2.4-2.	165
Figure 2.2.5-1.	170
Figure 2.2.5-2.	171
Figure 2.2.5-3.	188

Figure 2.2.6-1. [REDACTED]	194
Figure 2.2.7-1. [REDACTED]	201
Figure 2.2.7.2-1 [REDACTED]	207
Figure 2.2.8-1. [REDACTED]	211
Figure 2.2.8-2. [REDACTED]	217
Figure 2.2.8-3. [REDACTED]	223
Figure 2.2.8-4. [REDACTED]	228
Figure 2.2.8-5. TIC Portal Security Operations Center Architecture	229
Figure 2.2.8-6. [REDACTED]	235
Figure 2.2.8-7. [REDACTED]	240
Figure 2.2.8-8. [REDACTED]	251
Figure 2.2.8-9. [REDACTED]	262
Figure 2.2.8.7-1. [REDACTED]	269
Figure 2.2.8-9. [REDACTED]	274
Figure 2.2.8-10. [REDACTED]	275
Figure 2.2.8.9-1. [REDACTED]	284
Figure A-1-1. AT&T RMF Life Cycle	A-3
Figure A-2.1-1. [REDACTED]	A-10
Figure B-1-1. AT&T RMF Life Cycle	B-3
Figure B-2.1-1. [REDACTED]	B-9

LIST OF TABLES

Table 1-1. [REDACTED]	3
Table 1-2. Mapping RFP Sections C.1.1 through C.1.8.9 to the Proposal Response.	3
Table 1.1-1. [REDACTED]	5
Table 1.1-2. [REDACTED]	6
Table 1.1-3. [REDACTED]	10
Table 1.1.2-1. EIS Service Interoperability Definitions.	13
Table 1.1.3-1. [REDACTED]	14
Table 1.1.4-1. [REDACTED]	15
Table 1.1.5-1. SDN Technology Features and AT&T Future Plans.....	16
Table 1.1.5-2. NFV Technology Features and AT&T Future Plans.	17
Table 1.1.5-3. NFV/SDN Benefits.	18
Table 1.1.5-4. NFV/SDN Security and Standards.	18
Table 1.2.1-1. [REDACTED]	19
Table 1.2.2-1. [REDACTED]	19
Table 1.2.2-2. [REDACTED]	20
Table 1.2.3-1. [REDACTED]	20
Table 1.2.4-1. [REDACTED]	21
Table 1.3-1. [REDACTED]	26
Table 1.3-2. [REDACTED]	27
Table 1.4.3-1. [REDACTED]	34
Table 1.4.3-2. [REDACTED]	34
Table 1.4.3-3. [REDACTED]	35
Table 1.4.3-4. [REDACTED]	35
Table 1.4.3-5. [REDACTED]	36
Table 1.4.3-6. [REDACTED]	36
Table 1.4.3-7. Sensing and Control Mechanisms.....	36
Table 1.4.3-8. [REDACTED]	37
Table 1.4.3-9. [REDACTED]	37
Table 1.4.3-10. [REDACTED]	37
Table 1.4.4-1. [REDACTED]	38
Table 1.4.4-2. [REDACTED]	38
Table 2.1.1-1. [REDACTED]	40
Table 2.1.1-2. [REDACTED]	41
Table 2.1.1-3. [REDACTED]	43

Use or disclosure of data contained on this page is subject to the restriction on the title page of this document.

Table 2.1.4-5. [REDACTED]	92
Table 2.1.4-6. [REDACTED]	93
Table 2.1.4-7. [REDACTED]	94
Table 2.1.5-1. How AT&T Fulfills Section 508 Subparts B, C, and D.	97
Table 2.2.1-1. OWS Overview Description.	100
Table 2.2.1-2. OWS QoS.	101
Table 2.2.1-3. Approach to External Traffic Routing Requirements.	102
Table 2.2.1-4. OWS Service Scope and Functional Capabilities.	103
Table 2.2.1-5. OWS Technical Capabilities.	104
Table 2.2.1-6. [REDACTED]	105
Table 2.2.1-7. [REDACTED]	107
Table 2.2.1-8. PLS QoS.	108
Table 2.2.1-9. [REDACTED]	109
Table 2.2.1-10. [REDACTED]	110
Table 2.2.1-11. [REDACTED]	110
Table 2.2.1-12. [REDACTED]	111
Table 2.2.1-13. [REDACTED]	113
Table 2.2.1-14. [REDACTED]	114
Table 2.2.1-15. [REDACTED]	115
Table 2.2.1-16. [REDACTED]	116
Table 2.2.1-17. [REDACTED]	117
Table 2.2.1-18. [REDACTED]	118
Table 2.2.1-19. [REDACTED]	119
Table 2.2.1-20. [REDACTED]	121
Table 2.2.1-22. [REDACTED]	122
Table 2.2.1-23. [REDACTED]	122
Table 2.2.1-24. [REDACTED]	123
Table 2.2.1-25. [REDACTED]	125
Table 2.2.1-26. [REDACTED]	127
Table 2.2.1-27. [REDACTED]	128
Table 2.2.1-28. [REDACTED]	128
Table 2.2.1-29. IPS Service Scope and Functional Capabilities.	129
Table 2.2.1-30. [REDACTED]	130
Table 2.2.1-31. [REDACTED]	130
Table 2.2.1.6-1. [REDACTED]	132
Table 2.2.1.6-2. [REDACTED]	133
Table 2.2.1.6-3. [REDACTED]	133
Table 2.2.1.6-4. [REDACTED]	134

Table 2.2.1.6-5.		135
Table 2.2.1.6-6.		135
Table 2.2.1.6-7.		136
Table 2.2.2-1.		138
Table 2.2.2-2.		139
Table 2.2.2-4.		140
Table 2.2.2-5.		141
Table 2.2.2-6.		142
Table 2.2.2-7.		145
Table 2.2.2.2-1.		147
Table 2.2.2.2-2.		148
Table 2.2.2.2-3.		149
Table 2.2.2.2-4.		149
Table 2.2.2.2-5.		150
Table 2.2.2.2-6.		151
Table 2.2.3-1.		152
Table 2.2.3-2.		154
Table 2.2.3-4.		155
Table 2.2.3-5.		156
Table 2.2.3-6.	CCS Features.	159
Table 2.2.4-1.		164
Table 2.2.4-2.		164
Table 2.2.4-4.		166
Table 2.2.4-5.		167
Table 2.2.4-6.		168
Table 2.2.5-1.	Cloud Essential Characteristics.	169
Table 2.2.5-2.		171
Table 2.2.5-3.		172
Table 2.2.5-4.		173
Table 2.2.5-5.		174
Table 2.2.5-6.		175
Table 2.2.5-7.		175
Table 2.2.5-8.		177
Table 2.2.5.2-1.		178
Table 2.2.5.2-2.		178
Table 2.2.5.2-3.		179
Table 2.2.5.2-4.		180
Table 2.2.5.2-5.		181

Table 2.2.5.2-6.		182
Table 2.2.5.3-1.		183
Table 2.2.5.3-2.		184
Table 2.2.5.3-3.		184
Table 2.2.5.3-4.		185
Table 2.2.5.3-5.		186
Table 2.2.5.3-6.		187
Table 2.2.5-9.		188
Table 2.2.5-10.		189
Table 2.2.5-12.		190
Table 2.2.5-13.		191
Table 2.2.5-14.		192
Table 2.2.5-15.		192
Table 2.2.6-1.		194
Table 2.2.6-2.		195
Table 2.2.6-4.		196
Table 2.2.6-6.		199
Table 2.2.7-1.		201
Table 2.2.7-2.		202
Table 2.2.7-4.		203
Table 2.2.7-5.		204
Table 2.2.7-6.		205
Table 2.2.7.2-1.		207
Table 2.2.7.2-2.		208
Table 2.2.7.2-3.		209
Table 2.2.7.2-4.		209
Table 2.2.8-1.	WCS Overview Description.	211
Table 2.2.8-2.	WCS QoS.	212
Table 2.2.8-4.		213
Table 2.2.8-5.		214
Table 2.2.8-6.		216
Table 2.2.8-7.		217
Table 2.2.8-8.		219
Table 2.2.8-10.		220
Table 2.2.8-11.		220
Table 2.2.8-12.		223
Table 2.2.8-13.		225

Table 2.2.8-14.	226
Table 2.2.8-15.	227
Table 2.2.8-16.	229
Table 2.2.8-17.	231
Table 2.2.8-18.	233
Table 2.2.8-19.	236
Table 2.2.8-20.	237
Table 2.2.8-22.	238
Table 2.2.8-23.	241
Table 2.2.8-24.	245
Table 2.2.8-25.	251
Table 2.2.8-26.	252
Table 2.2.8-28.	253
Table 2.2.8-29.	254
Table 2.2.8-29a.	260
Table 2.2.8-30.	262
Table 2.2.8-31.	263
Table 2.2.8-33.	265
Table 2.2.8-34.	265
Table 2.2.8-35.	266
Table 2.2.8.7-1.	269
Table 2.2.8.7-2.	271
Table 2.2.8.7-3.	272
Table 2.2.8.7-4.	272
Table 2.2.8.7-5.	273
Table 2.2.8-36.	275
Table 2.2.8-37.	277
Table 2.2.8-38.	278
Table 2.2.8-39.	278
Table 2.2.8-40.	279
Table 2.2.8-41.	280
Table 2.2.8-42.	282
Table 2.2.8.9-1.	284
Table 2.2.8.9-2.	286
Table 2.2.8.9-3.	287
Table 2.2.8.9-4.	287
Table 2.2.8.9-5.	288
Table 2.2.8.9-6.	289

Table 2.2.8.9-7. [REDACTED]	290
Table 2.2.9-1. [REDACTED]	292
Table 2.2.9-2. [REDACTED]	292
Table 2.2.11-1. [REDACTED]	294
Table 2.3-1. [REDACTED]	295
Table 2.3-2. [REDACTED]	295
Table A-2.2-1. Operational Control Topics.	A-11
Table A-2.2-2. Technical Control Topics.	A-18
Table B-2.2-1. Operational Control Topics.	B-11
Table B-2.2-2. Technical Control Topics.	B-18
Table C-1-1. [REDACTED]	C-1

ABBREVIATION AND ACRONYM DEFINITIONS LIST

Abbreviation/Acronym	Definition
100G	100 Gb/s
3DES	Triple Data Encryption Standard
3G	Third Generation
4G	Fourth Generation
A&A	Assessment and Authorization
A&A	Authorization and Accreditation
AA	Access Arrangements
AAFES	Army and Air Force Exchange Service
AC	Access Control
ACD	Automated Call Distributor
ACS	Audio Conferencing Services
AD	Active Directory
ADA	Americans with Disabilities Act
ADM	Add Drop Multiplexing
ADSL	Asymmetric DSL (Digital Subscriber Line)
AES	Advanced Encryption Standard
AIC	AT&T Integrated Cloud
ALI	Address Location Information
AMI	Alternate Mark Inversion
ANI	Automatic Number Identification
ANSI	American National Standards Institute
AO	Authorizing Official
AOTDR	Automated Optical Time Domain Reflectometer
AOUSC	Administrative Office of the United States Courts
API	Application Programming Interface
APS	Automatic Protection Switching
APT	Advanced Persistent Threat
ARIN	American Registry for Internet Numbers
AS	Autonomous System
ASCII	American Standard Code for Information Interchange AMI and B8ZS Line code
ASN	Autonomous System Numbers
ASPR	AT&T Security Policy and Requirements
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
ATO	Authority to Operate
AU	Authorized Users
AUP	Acceptable Use Policy
AV	Audio Video
AVI	Audio Visual Interleave
AWG	American Wire Gauge
AWS	Amazon Web Services
AWS	Advanced Wireless Service
AWS-3	Advanced Wireless Service 3
B2Bi GW	Business to Business Integration Gateway
BCS	Business Communication Services
BFD	Bidirectional Forward Detection

Abbreviation/Acronym	Definition
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol Version 4
BIA	Business Impact Assessment
[REDACTED]	[REDACTED]
BLSR	Bidirectional Line Switched Ring
BoD	Bandwidth on Demand
BOE	Building of Entry
BRI	Basic Rate Interface
BSD	Boundary and Scope Document
BSS	Business Support System
BU	Business Unit
BU-EMC	Business Unit - Emergency Management Council
BURT	Business Unit Response Team
BYOD	Bring Your Own Device
CAD	Computer-Aided Design
CAS	Channel Associated Signaling
CBP	U.S. Customs and Border Protection
CBS	Committed Burst Size
CBWFQ	Class-Based Weighted Fair Queuing
CC	Control Center
CCS	Contact Center Service
CCV	Cybersecurity Compliance Validation
CDN	Content Delivery Network
CDNS	Content Delivery Network Service
CDR	Call Detail Record
CD-ROM	Compact Disk – Read Only Memory
CE	Customer Edge
CE-PE	Customer Edge – Provider Edge
CERT	Computer Emergency Readiness Team
[REDACTED]	[REDACTED]
CH/Conc	Channel/Concatenated
Ch/Unch	Channel/Unconcatenated
CHS	Colocated Hosting Service
CIO	Chief Information Officer
CIO-IT	Chief Information Officer – Information Technology
CIR	Committed Information Rate
CIS	Center for Internet Security
CLEC	Competitive Local Exchange Carrier
CM	Configuration Management
CMMI	Capability Maturity Model Integration
CMP	Configuration Management Plan
CMS	Call Management System
CNM	Customer Network Management
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CO	Contracting Officer
CO	Central Office
COE	Customer Owned Equipment

Abbreviation/Acronym	Definition
COMSATCOM	Commercial Satellite Communications Service
CONUS	Continental United States
COOP	Continuity of Operations Plan
CoS	Class of Service
COW	Cell on Wheel
CP	Contingency Plan
CPE	Customer Premises Equipment
CPTP	Contingency Plan Test Plan
CPTPR	Contingency Plan Test Plan Report
CPU	Central Processing Unit
CRAC	Computer Room Air Conditioning
CRM	Customer Relationship Management
CSC	Computer Sciences Corp.
CSDS	Circuit Switched Data Service
CSP	Cloud Service Provider
CSU	Channel Service Unit
CSU/DSU	Channel Service Unit/Data Service Unit
CSVS	Circuit Switched Voice Service
CTI	Computer Telephony Integration
CTW	Control Tailoring Workbook
CUI	Controlled Unclassified Information
CWS	Cable and Wiring Service
DAA	Designated Approving Authority
DACC	Digital Access Cross Connect
DB	Database
DBMS	Database Management System
DCS	Digital Cross-Connect Switch
DCS	Digital Cross-Connect System
DDoS	Distributed Denial of Service
DES	Design and Engineering Services
DFS	Dark Fiber Service
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DHTML	Dynamic Hyper Text Markup Language
DID	Direct Inward Dial
DISA	Defense Information Systems Agency
DKIM	Domain Keys Identified Mail
DMZ	Demilitarized Zone
DNCP	Dynamic Host Configuration Protocol
DND	Do Not Disturb
DNIS	Dialed Number Identification Service
DNS	Domain Name System
DNSSEC	Domain Name Systems Security Extensions
DOC	Department of Commerce
DoD	Department of Defense
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Network

Abbreviation/Acronym	Definition
DoE	Department of Energy
DOJ	US Department of Justice
DoS	Department of State
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DRS	Dedicated Ring Service
DS0	Digital Signal 0
DS1	Digital Signal 1
DS3	Digital Signal 3
DSB	Dual Stack Bearer
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSS	Data Security Standard
DSS	Decision Support Service
DSU	Data Service Unit
DSX	Digital Signal Cross-Connect
DTMF	Dual Tone Multifrequency
DWDM	Dense Wavelength Domain Multiplexer
DWDM	Dense Wavelength Domain Multiplexing
E	European
E&M	Ear and Mouth
ECC	Executive Command Council
ECV	Emergency Communications Vehicles
EIS RS	Electrical Industries Association Recommended Standard
EIS2020	Enterprise Infrastructure Solutions 2020
EIT	Electronic and Information Technology
E-LAN	Ethernet Private Local Area Network
ELEAF	Enhanced Leaf Fiber
ELIN	Electronic Library Information
E-LINE	Ethernet Private Line
EMC	Emergency Management Council
EMEA	Europe, the Middle East, and Africa
EMI	Electro-Magnetic Interference
EMO	Emergency Management Operations
EMP	Electromagnetic Pulse
ENNI	External Node-to-Node Interface
EoCu	Ethernet over Copper
EP	Emergency Preparedness
EPA	Environmental Protection Agency
EPLS	Ethernet Private Line Service
ERM	Email Response Management
ERP	Enterprise Resource Planning
ESCON	Enterprise System Connection
ESF	Extended Super Frame
ESI	Electronically Stored Information
ET	Earth Terminal
ETS	Ethernet Transport Service
ETSI	European Telecommunications Standards Institute

Abbreviation/Acronym	Definition
EVC	Ethernet Virtual Connection/Ethernet Virtual Channels
F/W	Firewall
FAA	Federal Aviation Administration
FASTAR	Fast Automatic Restoration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FD	Federal Document
FDP	Fiber Distribution Panel
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
FICON	Fiber Connectivity
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
FRR	Fast Re Route
FSDP	Fiber Service Delivery Point
FT3	Fractional T3
FTAS	Fiber Threat Analysis System
FTC	Federal Trade Commission
FTP	File Transfer Protocol
FTS	Federal Telecommunications Systems
FTTP	Fiber-to-the-Premise
FW	Firewall
GB	Gigabyte
GbE	Gigabit Ethernet
Gbps	Gigabits per Second
GCSC	Global Customer Support Centers
GETS	Government Emergency Telecommunications Service
GFE	Government Furnished Equipment
GFP	Government Furnished Property
GHG	Greenhouse Gas
GHz	Gigahertz
GIF	Graphics Interchange Format
GigE	Gigabit Ethernet
GNOC	Global Network Operation Center
GOS	Geospatial One-Stop
GPS	AT&T Global IP/MPLS Network Performance System
GPS	Global Positioning System
GR	Generic Requirement
GR-1230	Generic Requirement-1230
GR-253	Generic Requirement-253
GRC	Government, Risk, and Compliance
GRE	Generic Routing Encapsulation
GUI	Global Unique Identifier (TFS)
GUI	Graphical User Interface
GW	Gateway
HCM	Human Capital Management
HD	High Definition
HIPAA	Health Insurance Portability and Accountability Act

Abbreviation/Acronym	Definition
HP	Hewlett Packard
HS	High Speed
HSPA	High-speed Packet Access
HSPD	Homeland Security Presidential Directive
HSPD-12	Homeland Security Presidential Directive 12
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer/Transport Protocol
HTTPS	Hypertext Transfer/Transport Protocol Secure
HVAC	Heating, Ventilation, and Air Conditioning
I/O	Input/Output
IA	Information Assurance
[REDACTED]	[REDACTED]
IAR	Inbound Alternate Routing
IBM	International Business Machines
ICB	Individual Case Basis
ICD	Intelligence Community Directive
ICD-705	Intelligence Community Directive-705
ICMP	Internet Control Message Protocol
ID	Identifier
ID	Identification
IDC	Internet Data Center
IDE	Integrated Development Environment
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IDSL	IDSN Digital Subscriber Line
IDSL	Integrated Digital Subscriber Line
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IF	Interconnect Facilities
IF	Intermediate Frequency
iGEMS	AT&T Integrated Global Enterprise Management System
ILEC	Incumbent Local Exchange Carrier
ILEC	Independent LEC
IMEI	International Mobile Equipment Identity/Identification
IMM	Implementation Management and Maintenance
IMS	IP Multimedia Subsystem
INRS	Incident Reporting Service
InterLATA	Inter-Local Access Transport Area
IOC	Interoffice Connection
IoT	Internet of Things
IP	Internet Protocol
IPBE	IP Border Elements
IPS	Interoperability for Services
IPS	Intrusion Protection System
IPS	Internet Protocol Service
IPSec	Internet Protocol Security
IPSS	Intrusion Prevention Security Service
IPv6	Internet Protocol Version 6

Abbreviation/Acronym	Definition
IPVS	IP Voice Service/Internet Protocol Video Security
IR	Incident Response
IRP	Incident Response Plan
IRS	Internal Revenue Service
IRTR	Incident Response Test Report
ISA	Interconnection Security Agreements
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITILv3	Information Technology Infrastructure Library v3
ITO	Information Technology Office
ITSM	IT Service Management
ITU	International Telecommunications Union
IVR	Interactive Voice Response
IXC	Interchange Carrier/Channel
JAB	Joint Authorization Board
JUTNet	Justice Unified Telecommunications Network
K	Kilobit Per Second
KHz	Kilohertz
KPI	Key Performance Indicator
L2TP	Layer 2 Tunneling Protocol
L3	Layer 3
LAN	Local Area Network
LAS	Local Autonomous System
LATA	Local Access Transport Areas
LBI	Limited Background Investigation
LD	Long Distance
LDAP	Lightweight Directory Access Protocol
LEC	Local Exchange Carrier
LH	Long Haul
LLQ	Low Latency Queuing
LNP	Local Number Portability
LR	Long Reach
LSP	Label Switched Paths
LTE	Long-Term Evolution
M&Ps	Methods & Procedures
M2M	Machine to Machine
MAC	Moves Adds Changes
MACD	Moves Adds Changes and Disconnects
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MAS	Mobile Application Store
Mbps	Megabytes Per Second
MBS	Maximum Burst Size
MCM	Mobile Content Management

Abbreviation/Acronym	Definition
MD5	Message Digest Algorithm (128 bit) VJ
MDM	Mobile Device Management
MEF	Metro Ethernet Forum
MERS	Mobile Emergency Response Support
MGCP	Media Gateway Control Protocol
MHz	Megahertz
MIL-STD	Military Standard
MIMO	Multiple Input, Multiple Output
MLAN	Managed LAN
MLS	Managed LAN Service
MM	Mobility Management
MMF	Multimode Fiber
MMS	Multimedia Messaging Service
MMS	Managed Mobility Service
MNS	Managed Network Services
MOS	Mean Opinion Score
MOW	Most of World
MP	Media Protection
MPLS	Multiprotocol Label Switching
MRS-NOC	Managed Router Service – Network Operations Center
ms	Millisecond
MSPP	Multi Service Provisioning Platforms
[REDACTED]	[REDACTED]
MTA	Mail Transfer Agent
MTIPS	Managed Trusted Internet Protocol Service
MTU	Maximum Transmission Unit
[REDACTED]	[REDACTED]
N/A	Not Applicable
NAAR	Next Available Agent Routing
NAC	National Agency Check
NACI	National Agency Check with Written Inquiries
NANP	North American Numbering Plan
NARA	Network Application Readiness Assessment
NASA	National Aeronautics and Space Administration
NAT	National Address Translation
NB	Network Based
NBFW	Network Based Firewall
NCIC	National Crime Information Center
NCP	Network Control Point
NCP	Network Control Protocol
NCPS	National Cyber Protection System
NDR	Network Disaster Recovery
NE	Network Elements
NEBS	Network Equipment-Building System
NENA	National Emergency Number Association
NFV	Network Function Virtualization
NIST	National Institute of Standards and Technology
NOAA	National Oceanic and Atmospheric Administration

Abbreviation/Acronym	Definition
NOC	Network Operations Center
NoD	AT&T Network on Demand
NoSQL	Non SQL Database
NPA/NXX	Numbering Plan Area/Numbering Plan Exchange
NRC	Nuclear Regulatory Commission
NS	National Security
NS/EP	National Security/Emergency Preparedness
NSA	National Security Agency
NSOC	Network Security Operations Center
NTE	Network Terminating Equipment
NTP	Notice to Proceed
NXT	Nuclear Transport Factor 1
OC	Optical Carrier
OC-12	Optical Carrier 12
OC-192	Optical Carrier 192
OC-3	Optical Carrier 3
OC-48	Optical Carrier 48
OC-768	Optical Carrier 768
OCN	Optical Carrier Network
OCO	Ordering Contracting Officer
OCONUS	U.S. Territories and Possessions Outside the Contiguous 48 states
OCx	Object Linking and Embedding (OLE) custom control
ODU3	Optical Channel Data Unit 3
ODU4	Optical Channel Data Unit 4
OEC	Office of Emergency Communications
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplexing
OMB	Office of Management and Budget
OOB	Out of Band
OPNFV	Open Network Function Virtualization
OS	Operating System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSS	Operations Support Systems
OTN	Optical Transport Network
OTS	Optical Transport Systems
OVF	Open Virtualization Format
OWS	Optical Wavelength Service
[REDACTED]	[REDACTED]
PAT	Port Address Translation
Pb	Petrabyte
PBX	Private Branch Exchange
PC	Personal Computer
PCI	Payment Card Industry
PCL	Physical Concentration Location
PCS	Personal Communications Services
PCS	Personal Communications System
PDA	Personal Digital Assistants

Abbreviation/Acronym	Definition
PDH	Plesiochronous Digital Hierarchy
PDH/SDH	Plesiochronous Digital Hierarchy/Synchronous Digital Hierarchy
PDR	Packet Delivery Rate
PE	Provider Edge
PE	Physical and Environmental
PE-CE	Provider Edge-Customer Edge
PIA	Privacy Impact Assessment
PIM	Personal Information Management
PIN	Personal Identification Number
PING	Packet Internet Groper
PIR	Peak Information Rate
PKI	Public Key Encryption
PL	Programming Language/Private Line
PL	Planning
PL-IOC	Private Line/Interoffice Connection
PLS	Private Line Service
PLS/SONET/OWS	Private Line/Synchronous Optical Network/Optical Wave Service
PMI	Project Management Institute
PMOSS	Performance Management Operation Support System
POA&M	Plan of Action and Milestones (consistent w/acronym list in RFP)
POC	Point of Contact
POE	Power Over Ethernet
POM	Proactive Outreach Manager
PoP	Point of Presence
POP	Post Office Protocol
POSIP	Parallel Optical Interface
POTS	Plain Old Telephone Service
PPCoS	Per Packet Class of Service
PPP	Point-to-point Protocol
PRI	Primary Rate Interface
PS	Parallel Switched
PS	Private Switch
PS	Personnel Security
PSAP	Public Safety Answering Points
PSTN	Public Switched Telephone Network
PTT	Push to Talk
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RA	Risk Assessment
RADIUS	Remote Access Dial-In User Server
RAS	Replace Autonomous System
RC4	Rivest Cypher 4
RDBMS	Relational Database Management System
REV	Revision
RF	Radio Frequency
RFC	Remote Function Call/Radio Frequency Control
RFC-2361	Radio Frequency Code-2361
RFI	Radio Frequency Interference

Abbreviation/Acronym	Definition
RMF	Risk Management Framework
ROADM	Reconfigurable Optical Add/Drop-Multiplexers
RoB	Rules of Behavior
RPAS	Remove Private Autonomous System
RPP	Remote Power Panels
RS	Reduced Slope
RSVP	Resource Reservation Protocol
RTP	Real-time Transport Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions (IETF)
S/NOC	Security/Network Operations Centers
SA	Services Acquisition
SA&A	Security Assessment and Authorization
SAFER	Split Access Flexible Egress Routing
SAN	Storage Area Network
SAP	Security Assessment Plan
SAR	Security/Risk Assessment Report
SAS	Statement on Auditing Standards
SBA	Small Business Administration
SC	System and Communications
SCCP	Signaling Connection Control Part
SCI	Sensitive Compartmentalized Information
SCIF	Sensitive Compartmentalized Information Facility
SCN	Shared Component Nodes
SDD	System Design Document
SDDC	Software Defined Data Centers
SDH	Synchronous Digital Hierarchy
SDK	Software Development Kit
SDN	Software Defined Network/Networking
SDP	Service Delivery Point
SDSL	Symmetric DSL
SED	Service Enabling Device
SEIM	Security Event and Incident Management
SEN	Security Enforcement Node
SF	Super Frame
SF	Standard Form
SHA	Secure Hash Algorithm
SI	System and Information
SIEM	Security Information and Even Management
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SM	Single Mode
SMF	Single Mode (Optical) Fiber
SMPP	Short Message Peer to Peer
SMS	Short Message Service/System
SMS/MMS	Simple Network Management Protocol
SNMP	Short Message Service/System

Abbreviation/Acronym	Definition
SOAC	Security Operations Analysis Center
SOC	Security Operations Center
SOC1	Service Organization Control 1
SOC2	Service Organization Control 2
SOC3	Service Organization Control 3
SOHO	Small Office Home Office
SOMC	Security Operations Management Center
SON	Self Optimizing Networks
SONET	Synchronous Optical Network
SONETS	Synchronous Optical Network Service
SP	Special Publication
SPF	Sender Policy Framework
SQL	Structured Query Language
SR	Short Reach
SRE	Service Related Equipment
SRL	Service Related Labor
SS7	Signaling System 7
SSA	Social Security Administration
SSAE	Statement in Standards for Attestation Engagements
SSG	Satellite Solutions Group
SSL	Secure Sockets Layer/System Specifications Language
SSL/TLS	Secure Sockets Layer/Transport Layer Security
SSM	Synchronous Status Messaging
SSP	System Security Plan
ST	Straight Tip
ST&E	System Test Evaluation
STD	Standard
STS	Synchronous Transport Signal
SWC	Serving Wire Center
T1, T3	T-Carrier 1, T-Carrier 3
TACAC	Terminal Access Controller Access Control
TACACS	Terminal Access Controller Access Control System
TB	Terabyte
TCP	Transmission Control Protocol
TDM	Time Domain Multiplexing
TF	Toll Free
TFN	Toll Free Numbers
TFS	Toll Free Service
TIA-942	Telecommunications Industry Association (Standard)
TIC	Trusted Internet Connection
TL9000	Telecommunications Sector-specific ISO 9000
TLS	Transport Layer Security
TMS	Threat Management System
TO	Task Order
TOH	Transport Overhead
TS	Top Secret
TS/SCI	Top Secret/Sensitive Compartmented Information

Abbreviation/Acronym	Definition
TSP	Telecommunications Service Priority
TTS	Text to Speech
TTY	Teletypewriter
TVA	Tennessee Valley Authority
U.S.C.	United States Code
UC	Unified Communications
uCPE	Universal Customer Premises Equipment
UCS	Unified Communications Service
UDP	User Datagram Protocol
UIFN	Universal International Toll-Free Numbers
ULH	Ultra Long Haul
UM	Unified Messaging
UMTS	Universal Mobile Telecommunications Service
UNI	User to Network Interface
UPS	Uninterruptible Power Supply
UPSR	Unidirectional Path Switched Ring
URL	Universal Resource Locator
URL	Uniform Resource Locator
USAID	US Agency for International Development
US-CERT	United States Computer Emergency Readiness Team
USDA	US Department of Agriculture
VA	US Department of Veteran Affairs
vCE	Virtual Customer Edge Router
VESDA	Very Early Smoke Detection Apparatus
VLAN	Virtual Local Area Network
VM	Virtual Machines
VNF	Virtualized Network Function
VNIC	Virtual Network Internet Connection
VoIP	Voice over Internet Protocol/Package
VPAT	Voluntary Product Accessibility Template
VPE	Virtual Provider Edge Router
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPNS	Virtual Private Network Service
VRF	Virtual Private Network Routing and Forwarding
VS	Voice Service
VSR	Very Short Reach
VSS	Vulnerability Scanning Service
VT1.5	Virtual Tributary 1.5
VTs	Video Teleconferencing Service
WAN	Wide Area Network
WCS	Web Conferencing Service
WDM	Wavelength Division Multiplexing
WFM	Workforce Management
WFO	Work Force Optimization
WiFi	Wireless Fidelity
WPS	Wireless Priority Service
WS	Wireless Service



Abbreviation/Acronym	Definition
xDSL	Multiple Digital Subscriber Line
XML	Extensible Markup Language
YE	Year End



VOLUME 1 — [L.29; L.11; M.2.1; C.1; C.2; C.4]

1 Proposed Network Architecture [L.29(1); L.29.1; M.2.1]

General Services Administration (GSA)
customer agencies will benefit from our ongoing network investments, extensive suite of services, and skilled personnel for custom and highly-secure, mission-focused telecommunications and information technology (IT) solutions. These solutions will enable customer agencies to achieve mission goals faster, more effectively, and with fewer resources, now and over the life of the Enterprise Infrastructure Solutions (EIS) contract.

AT&T's EIS Solution Summary
Enabling Agency Missions through Innovative, Integrated, and Secured Enterprise Solutions
<ul style="list-style-type: none">■ Unrivaled global coverage & capacity■ Extensive solution offerings■ Best-value pricing commitments■ Cyber security expertise to anticipate and counter threats■ EIS transition expertise■ [REDACTED]

This section addresses the four evaluation criteria delineated in Request for Proposal (RFP) Section M.2.1:

- **Understanding:** The AT&T architecture reflects our understanding of both current and future federal needs. We meet current needs by offering [REDACTED] of the [REDACTED] EIS services. We will meet future needs by planning for emerging technologies, [REDACTED], which will enable agencies to respond to opportunities and threats with unprecedented agility.
- **Quality of Services:**
 - **Compliance:** Our architecture complies with the requirements of all 29 services we are bidding.
 - **Scalability:** The AT&T \$140B network investment over the last six years (2009 – 2014) demonstrates our ability to increase the scale of our architecture.
 - **Reliability:** The AT&T service [REDACTED].
 - **Resilience:** The AT&T core [REDACTED]. AT&T network business units each follow established response plans to address network events and have escalation paths to senior management as needed.

■ **Service Coverage:** We serve [REDACTED]. In total, AT&T proposes mandatory services in [REDACTED] of the [REDACTED] CBSAs. [REDACTED].

■ **Security:** The security architecture incorporates:

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

As the GSA conceived and deployed its Network Services 2020 (NS2020) strategy in support of its agency customers, it recognized that current and future technologies and solutions must be reliable, scalable, and highly secured to support the agencies' missions. Further, service solutions must be delivered ubiquitously to agency locations, whether domestic or abroad, with the ability to support users who are on site, remote, or mobile. To meet these challenges, GSA needs EIS contractors such as AT&T to provide highly secured, reliable, scalable, and competitively priced service solutions and support to its customer agencies worldwide.

AT&T has invested significantly in our network, service portfolio, and personnel, who design, develop, implement, and support the network and services.

Table 1-1 summarizes AT&T EIS service offerings, which result from a detailed assessment of the RFP requirements, and [REDACTED] that is highly reliable, highly resilient, highly secured, low-risk, comprehensive, global, highly scalable, and "future first". Additionally, AT&T is offering mandatory services in 99 of the [REDACTED]. We welcome the opportunity to continue delivery of our service solutions to the GSA and its customer agencies.

[illegible]

Table 1-2. Mapping RFP Sections C.1.1 through C.1.8.9 to the Proposal Response. *To facilitate the review of the proposals, this table maps RFP Sections C.1.1 through C.1.8.9 to our proposal response.*

RFP Section	Proposal Section or Subsection Name	Proposal Section
C.1.1	Proposed Network Architecture	1
C.1.2	Proposed Network Architecture	1
C.1.3	Proposed Network Architecture	1
	Geographic Coverage	1.1.1
	Service Coverage	1.3
C.1.4, C.1.5	Informational	N/A
C.1.6	Network Function Virtualization/Software-Defined Networking	1.1.5
C.1.7,C.1.8.1,C.1.8.2	Informational	N/A
C.1.8.3	Performance Metrics	2.1.1 – 2.1.3
	Performance Metrics	2.2.1 – 2.2.8

RFP Section	Proposal Section or Subsection Name	Proposal Section
C.1.8.4	Standards	2.1.1 – 2.1.3
		2.2.1 – 2.2.8
C.1.8.5	Voice Services	2.1.2
	Voice Services	2.2.2
	Service Coverage	1.3
	Interface; Performance Metrics	2.1.1 – 2.1.3
	Interface; Performance Metrics	2.2.1 – 2.2.8
C.1.8.6	Interoperability	1.1.2
	Connectivity	2.1.1 – 2.1.3
	Connectivity	2.2.1 – 2.2.8
C.1.8.7	Services Risk Management Framework	Appendix A
	MTIPS Risk Management Framework	Appendix B
	Security	2.1.1 – 2.1.3
	Security	2.2.1 – 2.2.8
C.1.8.8	NS/EP	1.1.3
	IPv6	1.1.4
	Security	1.4
	External Traffic Routing Requirements	2.1.1 – 2.1.3
	External Traffic Routing Requirements	2.2.1 – 2.2.8
C.1.8.9	Assumptions and Conditions	Assumptions and Conditions

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

Customer agencies will have access to a wireless and wireline network, tools, and personnel with a history of demonstrated performance in designing and implementing solutions in support of agency mission requirements and provide best-value through shared, cloud-based, and managed solutions. With the transition to an all-Internet Protocol (IP) network and SDNs, AT&T offers customer agencies the technology and tools to self-configure and modify their networks in real time and efficiently take advantage of emerging services. Over the next 15 years, agencies will demand advanced networks with the capability for continuous and non-disruptive performance improvements to achieve or exceed their missions. During this time, agencies will face multiple network transitions. Specifically, agencies will transition towards highly secured, managed, mobile, and wireline IP-based networks that integrate new and emerging cloud services. Agencies will use the new network architectures to create telecommunication solutions required for their missions. As carriers evolve to SDN, agencies will benefit from self-provisioned services and accelerated service delivery. **Table 1.1-1** provides a summary of the transition opportunities available to the agencies over the EIS contract life.



Table 1.1-1. Architecture Supports Agency Technology Requirements Now and In the Future. *The AT&T extensive network architecture supports agency needs, such as communications, data transport and IT applications.*

Technology	Description	Benefit to Agency
[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]	[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]



Technology	Description	Benefit to Agency

To embrace these network technologies, agencies require an offeror with a full service network. Agencies will benefit from the nearly \$140B investment AT&T made in our networks in the US over the last six years (2009-2014).

. Agencies will benefit from the AT&T intended investment over the next 15 years, knowing they will have access to a network that enables them to transition to future networking technologies. **Table 1.1-2** outlines AT&T network infrastructure available to the agencies.

Table 1.1-2. AT&T Network Addresses Agency Technology Needs Over the Next 15 Years.

Technology	AT&T Network	Benefit to Agency

[REDACTED]

Technology	AT&T Network	Benefit to Agency
[REDACTED]	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] 	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] 	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] 	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] 	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[illegible]

The scope, scalability, capacity, performance, security, and reliability of the AT&T network will reduce customer agency concerns about procuring complex enterprise services. Using the AT&T infrastructure, over the next 15 years, agencies will have access to enterprise services that best address their mission and a commitment from a single vendor that offers a full portfolio of [REDACTED] services designed, implemented, and supported by skilled and experienced personnel. **Figure 1.1-1** depicts how the AT&T network will support EIS services and **Table 1.1-3** describes the network capabilities we offer.

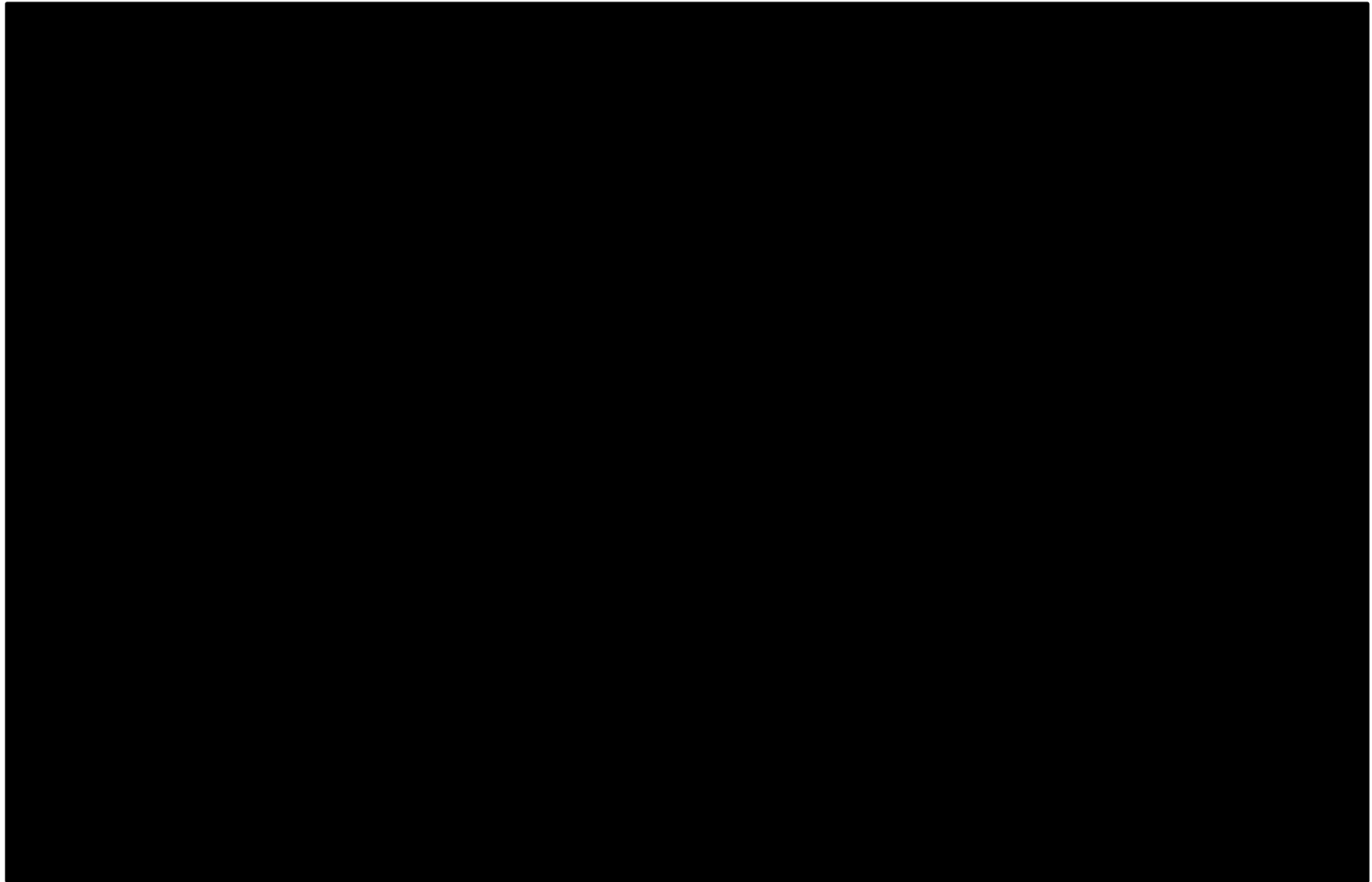


Figure 1.1-1. The AT&T Network: Infrastructure to Support Mandatory and Optional Services.

Table 1.1-3. AT&T Network Capabilities.

Network Component	Description and Details
Core Network	
	
	
	

Customer Interface

Network Component	Description and Details
[REDACTED]	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED]	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

1.1.1 Geographic Coverage [C.1.2; C.1.3]

[REDACTED]

[REDACTED] **Section 2.1.1.1;** [REDACTED] **Section 2.1.1.2;** [REDACTED]

[REDACTED] **Section 2.1.2.1 and Section 2.1.2.2;** MNS [REDACTED]

Section 2.1.3.1; [REDACTED] **Section 2.1.4.1.**

AT&T is offering mandatory services in [REDACTED]

[REDACTED]

Section 1.3.

1.1.2 Interoperability [C.1.8.6]

Customer agencies will receive AT&T commercially available service interoperability with performance equal to that provided for commercially available services and will be able to communicate from our network to other EIS contractor networks with equivalent performance where commercial interoperability exists.

Moreover, AT&T:

- Will support connectivity and interoperability for remote and mobile users for all proposed individual services, including between voice services and wireless services, as applicable.
- Will enable a user of a service from AT&T to communicate with users of services from other EIS contractors with equivalent performance.
- Will make available any future service interoperability at no additional cost to GSA when AT&T offers the interoperability for its commercially provided service

The EIS services interoperability are described in **Table 1.1.2-1**.

Table 1.1.2-1. EIS Service Interoperability Definitions. *EIS Service Interoperability alignment is categorized in the four interconnect methods as described below.*

Interoperability Definitions	Definition
PSTN	The EIS service uses PSTN interconnects for interoperability between services, [REDACTED]
Internet	The EIS service uses the public Internet for data interoperability for services [REDACTED]
Layer 1/layer 2	The EIS service interconnects with other vendors' EIS service at the Layer 1 (physical layer), or Layer 2 (data link layer). [REDACTED]
Dependent service	The EIS service is defined as a dependent service if it relies on a PSTN Interoperability, or an Internet interoperability service, [REDACTED]

1.1.3 National Security Emergency Preparedness (NS/EP) [C.1.8.8]

Government agencies can accomplish critical missions under the most challenging natural and man-made circumstances with the AT&T continued commitment to providing a full set of national security and emergency preparedness (NS/EP) services. In the event of crisis or nonstandard events, AT&T will provide a resilient network with

Table 1.1.3-1. NS/EP Suite of Services.

[illegible]

AT&T has a long history of working with IPv6, [REDACTED]

[REDACTED]

The AT&T MPLS network core is [REDACTED]

Table 1.1.4-1. [REDACTED]

[REDACTED].

[REDACTED]

The telecommunications industry is undergoing rapid, ongoing transformation in how applications are transported, how networks are deployed and managed, how services are secured, and how users interact with their service providers. Enterprise data networks are evolving from static pipes delivering packets to application-aware services capable of delivering real-time, On-Demand, network-based services. The AT&T goal is to [REDACTED] to simplify network provisioning and management for enterprise IT departments, and to deploy service when and where required.

1.1.5.1 Software Defined Network (SDN) [C.1.6]

SDN is an architectural framework that allows the network to transform into a more effective mission enabler. **Figure 1.1.5-1** presents the SDN architecture that demonstrates how software is used to decouple hardware from the network services. As the first telecommunications service provider to bring SDN-enabled features to the US by enabling dynamic bandwidth on AT&T switched Ethernet, [REDACTED]

[REDACTED]. **Table 1.1.5-1** presents the features, benefits, and future of SDN.

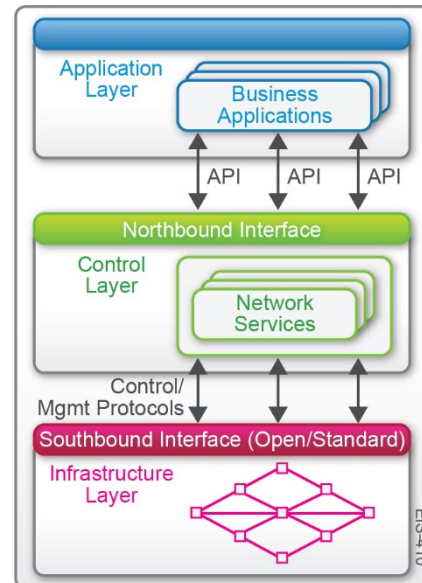
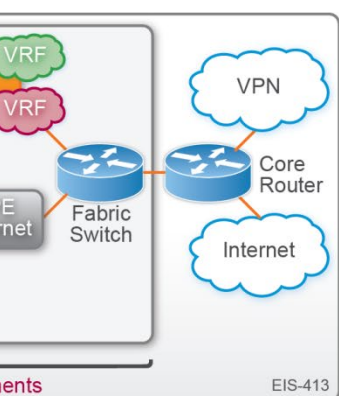


Figure 1.1.5-1. [REDACTED]

Table 1.1.5-1. SDN Technology Features and AT&T Future Plans. *With SDN, agencies will have more control of the network and the applications will dynamically request and receive network services.*

Focus Area	Features
SDN technology	<ul style="list-style-type: none"> ■ Separates the control plane, which contains the network configuration model, from the packet-forwarding infrastructure plane ■ Creates intelligent programmable networks that are more automated, application aware and open; ■ Uses APIs for applications and network management platform to communicate with control plane ■ Provides capability whereby applications request and manipulate network services and the network provides reporting data back ■ Uses High-level SDN controller languages, made accessible via AT&T SDN architecture, to simplify network configuration, ease the introduction of policy control, reduce errors, and enable more real-time changes in the network ■ Avoids wholesale replacement of existing network architectures; SDN leverages and augments the existing network routing control systems ■ Provides a global view of the entire network rather than a single point of view from one position ■ Enables distributed and dynamic routing control plane coupled with the centralized view to provide faster recovery in the event of a failure, and faster introduction of services into the network
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

ctions such as routers, country-standard high-speed data centers, network gateways, and so on, are distributed in various network locations. The network will also distribute the data, thereby eliminating the use of a central server. The virtual network is a key feature of the network. **Table 1.1.5-2**



former premises and PE are
connects with VNFs
ages immediately.

can add and remove network appliances.

dedicated hardware devices.
atches and upgrades, and
res.
artments to respond faster to
pital investment.
es without new hardware

1.1.5.3 NFV/SDN Benefits [C.1.6]

NFV/SDN together provide more competitively priced solutions as described in **Table 1.1.5-3**. Tighter integration with agencies' applications will improve customer productivity as shown in **Figure 1.1.5-3**. Simplified management will reduce the time and resources required for agencies to monitor, analyze, and plan for future changes to their networks.

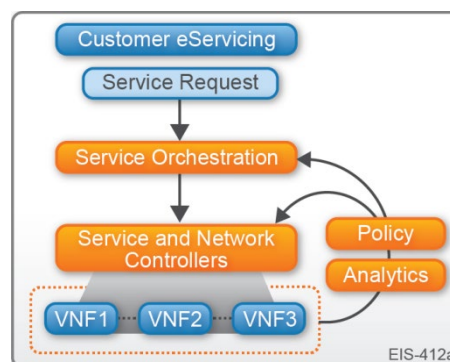


Figure 1.1.5-3. Service Model for an SDN with NFV. Service changes can be made through software-based policy and analytics can be applied to further automate service changes.

Table 1.1.5-3. NFV/SDN Benefits. With NFV/SDN, agencies will have more control of the network and their applications will dynamically request and receive network services.

NFV/SDN Benefits	
■ Control Planes:	By creating multiple, virtual network control planes on common hardware, SDN extends service virtualization and software control into existing network elements.
■ Applications:	Enables layers 4-7 applications to request network services and receive the network state back.
■ Services:	Allows applications' and management platforms' control of network services through APIs.
■ Access:	Provides access through remotely controlling network equipment and modifying network equipment via third-party software clients.
■ Control:	Logically decouples network intelligence into differentiated software-based controllers; flexibility provides a more centralized layer of control with a more global network view, improving control plane algorithms.

1.1.5.4 NFV/SDN Security and Standard [C.1.6]

As described in **Table 1.1.5-4**, security will improve as networks migrate to an NFV/SDN environment, while AT&T support for standards will help enable agencies to operate multi-vendor networks.

Table 1.1.5-4. NFV/SDN Security and Standards. Agencies will access more security services in real time. Participations in standards groups is essential for supporting multi-vendor NFV/SDN solutions.

NFV/SDN	Implementation
Security	<ul style="list-style-type: none"> ■ SDN control layer enables uniform security policies across services. ■ SDN enables deployment of additional security measures in real time. ■ NFV/SDN-based networks will include: <ul style="list-style-type: none"> — Role-based access controls that authenticate users for access to IT services — On-demand security features, such as network-level encryption across the WAN — Modular security solutions that combine security solutions from multiple vendors — Automated security patching — Reduced administration and management burden due to use of virtual machines — Services associated with perimeter security deployed at the node level, with policies specific to the node, providing stronger risk mitigation for agency applications
Standards	<ul style="list-style-type: none"> ■ AT&T participates in, and contributes to numerous industry and standards organizations. ■ AT&T is leveraging our unique expertise as a global, at-scale, reliable carrier in the SDN. ■ AT&T has leadership roles in European Telecommunications Standards Institute (ETSI) NFV working groups, OpenStack, Open Network Function Virtualization (OPNFV), TM Forum, and Internet Engineering Task Force (IETF).

This section presents the compliance, scalability, resilience, and reliability of our network architecture.

Table 1.2.1-1 summarizes compliance of the network architecture.

To enable agencies to scale their telecommunications networks to the capacity required over the next 15 years, AT&T provides one of the largest, scalable, global telecommunications networks, a growing number of carefully vetted companies, and highly experienced personnel. These assets will enable AT&T to plan and execute telecommunications growth at a scale that exceeds the agencies' needs into the future.

_____.

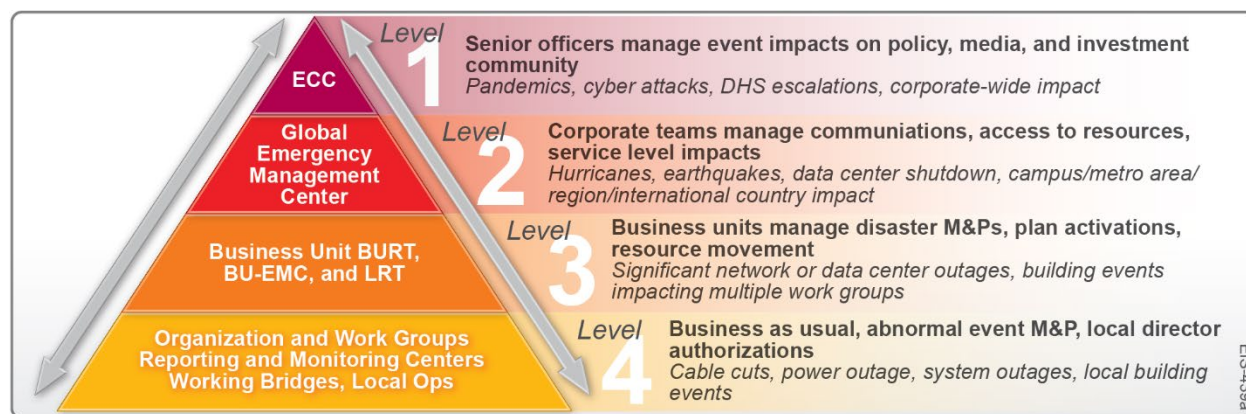
[illegible]

Premises edge	Access Redundancy Available when Required: <ul style="list-style-type: none"> Single access line arrangement Ring-based access arrangement Dual access lines arrangement 		

[illegible]

[illegible]

Defining roles and responsibilities and decision-making authority at the corporate, BU, and local levels enables network events to be managed effectively. AT&T has implemented an event management framework that provides an efficient and orderly recovery and restoration process. The framework uses the continuous assessment and action refinement methodology shown in **Figure 1.2.5-1**.



2004-01-01

1.2.6 Network Disaster Recovery

AT&T developed its Network Disaster Recovery (NDR) capability specifically for rapid service recovery during a wide range of disaster scenarios. NDR provides business continuity and recovery capabilities for the AT&T Global Network.

One of the primary roles of the AT&T NDR organization is to recover the services of an AT&T network office that has been completely destroyed or compromised by a natural or man-made disaster. **Figure 1.2.6-1**

Figure 1.2.6-1. NDR Site in Jersey City, NJ, September 2001.

The AT&T NDR team includes AT&T managers, engineers, and technicians who have received special training in the physical recovery of AT&T networks.

The NDR Team establishes broadband and wireless voice and data connectivity from disaster

Figure 1.2.6-2

Figure 1.2.6-2. NDR COW.

1.3 Service Coverage (CBSA-Dependent Services) [L.29.1(C); M.2.1(3); C.1.3]

AT&T offers GSA an extensive global network and service delivery

in order for AT&T to offer services at additional locations through our expanding network. Domestically, AT&T proposes

(as listed in Table 1-1).

We provided specific details of service coverage in Table 1.3-1 for CBSAs and in Table 1.3-2 for non-domestic countries and OCONUS.

[illegible]

[illegible]

120078	■				■						■							
120079	■																	
120080	■																	
120302					■						■							
120081	■				■		■			■	■		■					
120082	■				■						■							
120083																		
120084																		
120085	■				■					■	■		■					
120086	■																	
120266	■																	
120087	■																	
120088					■						■							
120089	■				■						■							
120143	■																	
120090	■				■						■							
120091																		
120303					■						■							
120304					■					■	■							
120093	■				■					■	■		■					
120094	■				■					■	■		■					
120095					■						■							
120096	■																	
120097	■				■						■							
120098	■				■						■							
120305					■						■							
120099																		
120100	■				■						■							
120101	■				■						■		■					
120102	■				■						■							
120103	■																	
120104					■						■							
120105	■				■						■							
120106	■				■						■							
120107																		
120108																		
120109					■						■							
120110	■				■					■	■		■					
120111	■				■		■			■	■		■					
120112	■				■						■							
120113					■						■							
120114																		
120314																		
120115	■				■						■							
120116	■				■						■							
120117	■				■						■							
120118	■				■		■			■	■		■					
120119	■				■						■							
120120					■						■							
120121	■				■					■	■		■					

120122																		
120123																		
120124																		
120126																		
120127																		
120129																		
120128																		
120130																		
120131																		
120132																		
120133																		
120134																		
120135																		
120136																		
120137																		
120138																		
120139																		
120140																		
120141																		
120142																		
120144																		
120145																		
120146																		
120147																		
120148																		
120149																		
120306																		
120152																		
120153																		
120154																		
120155																		
120156																		
120157																		
120158																		
120159																		
120160																		
120161																		
120162																		
120163																		
120164																		
120165																		
120166																		
120167																		
120168																		
120169																		
120170																		
120310																		
120172																		
120173																		
120174																		

180020																		
120178																		
120179																		
120180																		
120320																		
120181																		
120182																		
120183																		
120072																		
120184																		
120185																		
120186																		
120187																		
120188																		
120032																		
120189																		
120190																		
120191																		
120192																		
120193																		
120194																		
120195																		
120150																		
120196																		
120197																		
120198																		
120307																		
120200																		
120201																		
120202																		
120203																		
120204																		
120205																		
120206																		
120207																		
120208																		
120209																		
120210																		
120211																		
120212																		
120264																		
120219																		
120220																		
120221																		
120222																		
120223																		
120224																		
120225																		
120226																		
120227																		

120228																		
120229																		
120230																		
120231																		
120151																		
120272																		
120232																		
120233																		
120213																		
120214																		
120215																		
120216																		
120217																		
120234																		
120235																		
120236																		
120237																		
120238																		
120239																		
120240																		
120241																		
120242																		
120243																		
120244																		
120308																		
120245																		
120246																		
120247																		
120248																		
120249																		
120250																		
120251																		
120252																		
120253																		
120254																		
120255																		
120256																		
120257																		
120258																		
120312																		
120259																		
120260																		
120262																		
120263																		
120265																		
120267																		
120318																		
120268																		
180025																		
180026																		

180027																		
180029																		
180036																		
180037																		
180038																		
180039																		
180040																		
180041																		
180042																		
180043																		
180044																		
180045																		
180046																		
180047																		
180048																		
180049																		
OCONUS Country ID																		
179627																		
120270																		
120269																		
120171																		
120176																		
120177																		
120199																		
120317																		
120261																		
120036																		
120037																		
120316																		

Agencies will have the ability to better achieve their missions globally through the AT&T network geographic reach.

1.4 Security [L.29.1(D); L.11; M.2.1(4)]

Customer agencies will receive a fully compliant security architecture that includes

1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

Section 2

1.4.2 General Requirements Described in Sections C.1.8.7 [M.2.1(4)(b); C.1.8.7]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1.4.3 External Traffic Routing Requirements [L.29.2.3; M.2.1(4)(c); C.1.8.8]

GSA requires an overall security architecture to meet agency traffic routing conditions.

Figure 1.4.3-1 [REDACTED]

[REDACTED]

[REDACTED]

Table 1.4.3-1.

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

Figure 1.4.3-1. Trusted Internet Connection (TIC) and National Cyber Protection System (NCPS) Support.

	2019	2020	2021
1. Revenue			
2. Expenses			
3. Net Income			
4. Assets			
5. Liabilities			
6. Equity			
7. Other			
8. Total			

Category	Item	Value
Category 1	Item 1.1	Value 1.1
	Item 1.2	Value 1.2
	Item 1.3	Value 1.3
Category 2	Item 2.1	Value 2.1
	Item 2.2	Value 2.2
	Item 2.3	Value 2.3
Category 3	Item 3.1	Value 3.1
	Item 3.2	Value 3.2
	Item 3.3	Value 3.3

Table 1.4.3-3 describes the methodology for identifying participating agency traffic for each affected service.

[illegible]

1.4.3.2 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 [L.29.2.3(2); M.2.1(4)(c)(ii); C.1.8.8]

Table 1.4.3-4.

[illegible]

1.4.3.3 Technical Approach to Notify DHS If Any Non-Participating Agency Traffic Will Be Redirected Through DHS EINSTEIN Enclaves [L.29.2.3(3); M.2.1(4)(c)(iii)]

Table 1.4.3-5 describes the technical approach to notify DHS of redirecting traffic through DHS EINSTEIN Enclaves.

Table 1.4.3-5. Technical Approach for Notifying DHS of Redirected Traffic.

Component	Description
Agency demarcation	<ul style="list-style-type: none"> Defining a clear agency demarcation point is one of the steps to the technical approach for notifying DHS of redirecting traffic through an EINSTEIN Enclave.
VPN routes	<ul style="list-style-type: none"> Redirecting traffic through the DHS EINSTEIN Enclave is also achieved by defining and setting up specific VPN routes from the agency demarcation point, through the routing equipment in the agency colocation space, and onto the EINSTEIN Enclave as shown in Figure 1.4.3-1.
Extranet	<ul style="list-style-type: none"> We can determine, from an extranet, if non-participating agency traffic lands in a different agency's demarcation point. We will assist the participating agency to alert DHS that non-participating agency traffic will be routed through an EINSTEIN Enclave.

1.4.3.4 Control Mechanisms to Ensure the Identification and Redirection of Participating Agency Traffic Cannot Be Inadvertently or Maliciously Bypassed [L.29.2.3(4); M.2.1(4)(c)(iv)]

Table 1.4.3-6

against inadvertent or malicious bypass.

Table 1.4.3-6. Control Mechanisms.

Component	Description
Demarcation	<ul style="list-style-type: none"> Identify the demarcation point of the agency system, such as a router and firewall, where agency traffic is offloaded to the AT&T network
System access	<ul style="list-style-type: none"> Define which AT&T individuals have access to the system and what those individuals can access on the EINSTEIN Enclave, based on NIST Special Publication (SP) 800-53 physical and logical security access controls for a FISMA High system If necessary, perform a full FISMA High authorization on the agency security boundary to assess and expose any vulnerabilities that would allow malicious bypass of agency traffic and allow an agency to mitigate those vulnerabilities

1.4.3.5 Sensing and Control Mechanisms AT&T Will Use to Ensure the Redirection of Traffic is Failsafe Should Failures Occur with DHS GFP [L.29.2.3(5); M.2.1(4)(c)(v)]

Table 1.4.3-7 describes sensing and control mechanisms for fail-safe traffic redirection.

Table 1.4.3-7. Sensing and Control Mechanisms

1.4.3.6 Location of AT&T Existing or Planned ANSI/PIA-942 and ICD 705 Certified Facilities That Can Service as DHS EINSTEIN Enclaves Capable of Posting DHS GFP At Or Near Appropriate Traffic-Access Locations [L.29.2.3(6); M.2.1(4)(c)(vi)]

Table 1.4.3-8

Table 1.4.3-8. AT&T -Certified Facilities.

1.4.3.7 Availability of TS/SCI Cleared Personnel for “Smart-Hands” Service of DHS Supplied Equipment [L.29.2.3(7); M.2.1(4)(c)(vii)]

Table 1.4.3-9 describes the availability of TS/SCI cleared personnel to provide “Smart-Hands” service.

Table 1.4.3-9. AT&T Cleared Personnel. DHS can call on AT&T to provide cleared personnel to perform host administrative tasks on DHS-supplied equipment.

1.4.3.8 Instrumentation to Measure Transport of SLA KPIs [L.29.2.3(8); M.2.1(4)(c)(viii); C.1.8.8]

Table 1.4.3-10

Table 1.4.3-10. AT&T Measuring Transport SLA KPIs.

[illegible]

1.4.4.1 Detailed Technical Description [L.29.2.3; C.1.8.8]

1.4.4.1 Detailed Technical Description [L.29.2.3; C.1.8.8]

■ [REDACTED] Table 1.4.3-2

■ [REDACTED]

[REDACTED]

Table 1.4.4.1. Implementation of Aggregation Service. [REDACTED]

Component	Description
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>
	<div> <div></div> <div></div> </div>
	<div> <div></div> <div></div> </div>
	<div> <div></div> <div></div> </div>
	<div> <div></div> <div></div> </div>
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>
<div> <div></div> <div></div> </div>	<div> <div></div> <div></div> </div>

Our aggregation service operation is described below in **Table**

Table 1.4.4-2. Operation of Aggregation Service. *Agencies can implement and operate the*

Responsibility	Description
----------------	-------------

Responsibility	Description
[REDACTED]	[REDACTED]
	[REDACTED]
	[REDACTED]
[REDACTED]	[REDACTED]
	[REDACTED]

2 Technical Response [L.29(2); L.29.2; M.2.1; C.1; C.2]

This section of our proposal addresses the specific RFP requirements for individual mandatory and optional services. To aid GSA in its evaluation, we have organized our technical response for each mandatory and optional service using a common topical structure and tabular format. In addition to the response provided for each service, AT&T will provide customer technical support as a component of each of its EIS services.

2.1 Mandatory EIS Services [L.29(2)(a); L.29.2.1; M.2.1; C.1.2]

AT&T will offer GSA mandatory

. Our proposal response addresses all services defined as mandatory in RFP Section C. Our response describes how AT&T will provide the proposed services and features, including how AT&T will provide the service architecturally and technically (referencing the network architecture description provided in RFP Section L.29.1), and identifies solutions for the following areas (as defined in RFP Section M.2.1) for each proposed service: A. Understanding; B. QoS; C. Service Coverage (for CBSA-dependent services); and D. Security. For each proposed service, AT&T also indicates whether or not (and how) we will meet or exceed the following, as applicable: Service and Functional Description, Standards, Connectivity, Technical Capabilities, Features, Interfaces, and Performance Metrics.

2.1.1 Service Area: Data Service [C.2.1]

2.1.1.1 Virtual Private Network Service [L.29.2.1; M.2.1; C.2.1.1]

Customer agencies will be able to easily interconnect their sites across metropolitan areas or around the globe using AT&T Virtual Private Network Services (VPNS). The AT&T VPNS is an

a wide

AT&T VPNS is a secured private network foundation that delivers core connectivity to these powerful cloud-accessible services proposed:

■		■	
■		■	
■		■	
■		■	

range of connectivity options and features, [REDACTED]

2.1.1.1.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.1.1.1.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

With the AT&T proposed solution for VPNS, agencies will receive a highly secured, private IPv4/v6 networking solution through multiple access options. Managed and unmanaged VPNS options will offer agencies direct/remote access to network connected applications.

The AT&T VPNS will provide agencies access to our global MPLS backbone network, available in [REDACTED] countries, to develop a private and highly secured approach to transporting their multi-service IP traffic between sites.

The AT&T VPNS will offer agencies the flexibility to establish the following three required solutions as depicted in **Table 2.1.1-1**.

Agencies benefit from AT&T position as Market Leader. Examples include:

- AT&T received 2014 MPLS/IP VPN Services Market Leadership award... "in recognition of AT&T's ability to capture the largest market share in MPLS/IP VPN market, by strategically investing its resources to tap market potential for layer 3 VPN services..." (Frost & Sullivan, January 2015)
- AT&T identified as "One of the strongest Managed Global MPLS Service offerings" by Forrester Research, Inc.
- Frost & Sullivan remarks: "AT&T dominates the Business Communication Services (BCS) space with the highest revenue share in each of the network services and application segments, largely owing to its expansive network footprint, and the completeness of solutions it offers."

Table 2.1.1-1. [REDACTED]

Intranet, extranet, and remote access agencies users.

VPNS Req'd Service	Description of AT&T Solution
Intranet service	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]
Extranet service	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]
Remote access	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]

As depicted in **Figure 2.1.1-1** and **Table 2.1.1-2**, the AT&T proposed architecture and services will meet EIS service requirements.



Figure 2.1.1-1. VPNS Overview.

Table 2.1.1-2. VPNS Overview Description. *VPNS components support a rich set of IP-based services and function as the underlying/foundational network connectivity for remote users, access to cloud service providers, and centrally-controlled Internet access via network based firewall support.*

Architectural Components	Description
Functional Components	
Remote access	
Application gateways	
Firewall/filtering	
Technical Components	
Global MPLS network	
IPv4/IPv6 compatible	
Class of service	
Autonomous System (AS) support options	

Architectural Components	Description
Virtual Network Internet Connection (VNIC)	<ul style="list-style-type: none"> Virtual Network Interface Card (VNIC) connects the virtual machine to the physical network. Virtual Network Interface Card (VNIC) connects the virtual machine to the physical network.
Multicast virtual private network	<ul style="list-style-type: none"> Multicast virtual private network (VLAN) connects the virtual machine to the physical network. Multicast virtual private network (VLAN) connects the virtual machine to the physical network.
Bidirectional Forward Detection (BFD)	<ul style="list-style-type: none"> Bidirectional Forward Detection (BFD) connects the virtual machine to the physical network. Bidirectional Forward Detection (BFD) connects the virtual machine to the physical network.
MD5 hash	<ul style="list-style-type: none"> MD5 hash connects the virtual machine to the physical network. MD5 hash connects the virtual machine to the physical network.
Large Maximum Transmission Unit Support (MTU)	<ul style="list-style-type: none"> Large Maximum Transmission Unit Support (MTU) connects the virtual machine to the physical network. Large Maximum Transmission Unit Support (MTU) connects the virtual machine to the physical network.
Operational Components	
AT&T Integrated Global Enterprise Management System (iGEMS)	<ul style="list-style-type: none"> AT&T Integrated Global Enterprise Management System (iGEMS) connects the virtual machine to the physical network. AT&T Integrated Global Enterprise Management System (iGEMS) connects the virtual machine to the physical network.
Business center	<ul style="list-style-type: none"> Business center connects the virtual machine to the physical network. Business center connects the virtual machine to the physical network.
Managed Services	<ul style="list-style-type: none"> Managed Services connects the virtual machine to the physical network. Managed Services connects the virtual machine to the physical network.
Service level agreement	<ul style="list-style-type: none"> Service level agreement connects the virtual machine to the physical network. Service level agreement connects the virtual machine to the physical network.
Diversity	<ul style="list-style-type: none"> Diversity connects the virtual machine to the physical network. Diversity connects the virtual machine to the physical network.
Global support centers	<ul style="list-style-type: none"> Global support centers connects the virtual machine to the physical network. Global support centers connects the virtual machine to the physical network.
Network Components	
Core routers	<ul style="list-style-type: none"> Core routers connects the virtual machine to the physical network. Core routers connects the virtual machine to the physical network.
Customer edge and provider edge routers	<ul style="list-style-type: none"> Customer edge and provider edge routers connects the virtual machine to the physical network. Customer edge and provider edge routers connects the virtual machine to the physical network.
Access circuit	<ul style="list-style-type: none"> Access circuit connects the virtual machine to the physical network. Access circuit connects the virtual machine to the physical network.

— Wireless 3G/4G

2.1.1.1.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

As delineated in **Table 2.1.1-3**, our approach and architecture for providing VPNS will deliver compliant, scalable, reliable, and resilient service.

Table 2.1.1-3. VPNS QoS. VPNS is fully compliant and provides the robust scalability, high reliability, and strong resilience sought by GSA and customer agencies.

Architectural Components	Description
Compliance	
Demonstrated capability	<ul style="list-style-type: none"> Compliance with all applicable laws, regulations, and standards.
MPLS	
Global network	<ul style="list-style-type: none"> Global network coverage.
Network management	
Network control	<ul style="list-style-type: none"> Network control and management.
Data separation	<ul style="list-style-type: none"> Data separation and security.
No single point of failure (Core)	
Power backup	<ul style="list-style-type: none"> Power backup and redundancy.
Disaster recovery	<ul style="list-style-type: none"> Disaster recovery and business continuity.
High availability	<ul style="list-style-type: none"> High availability and uptime.

2.1.1.1.1.3 Service Coverage (CBSA-Dependent) [L.29.2.1(C); M.2.1(3); C.1.3]

See **Section 1.3** for AT&T service coverage for VPNS.

2.1.1.1.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.1.1.1.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

While VPNS has no service-specific requirements indicated in the RFP, **Table 2.1.1-4** delineates additional service-specific security capabilities delivered to agencies.

Table 2.1.1-4. VPNS Service-Specific Security Capabilities. Agencies using AT&T VPNS will benefit from the inherent security measures attributed to the MPLS architecture at the foundation of our global network.

Capability	Description
MPLS architecture security	[REDACTED]
Facility security standards	[REDACTED]
PCI compliance	[REDACTED]
Network-based firewall service	[REDACTED]

2.1.1.1.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency VPNS customers will be protected from information breaches, unauthorized access, and supply chain risks [REDACTED]

2.1.1.1.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3)]

As delineated in **Table 2.1.1-5**, our proposed architecture will meet all external traffic routing requirements applicable to VPNS.

Table 2.1.1-5. Approach to External Traffic Routing Requirements.

Requirement	Compliance Description
Methodology for Identifying AT&T Participating Agency Traffic for Each Affected Service [M.2.1.4.c.i].	[REDACTED] Section 1.4.3.1.
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 [M.2.1.4.c.ii]	[REDACTED] Section 1.4.3.2.
Technical Approach to Notify DHS If Any Non-Participating Agency Traffic Will Be Redirected Through DHS EINSTEIN Enclaves [M.2.1.4.c.iii]	[REDACTED] Section 1.4.3.3.

Requirement	Compliance Description
Control Mechanisms to Ensure the Identification and Redirection of Participating Agency Traffic Cannot Be Inadvertently or Maliciously By-Passed [M.2.1.4.c.iv]	Section 1.4.3.4.
Sensing and Control Mechanisms to Ensure the Redirection of Traffic is Fail Safe [M.2.1.4.c.v]	Section 1.4.3.5.
Location of AT&T Certified Facilities [M.2.1.4.c.vi]	Section 1.4.3.6.
Availability of TS/SCI Cleared Personnel for “Smart-Hands” Service of DHS Supplied Equipment [M.2.1.4.c.vii]	Section 1.4.3.7.
Instrumentation to Measure Transport SLA KPIs [M.2.1.4.c.viii]	Section 1.4.3.8.

2.1.1.1.2 Technical Response for VPNS [L.29.2.1; M.2.1]

2.1.1.1.2.1 Service Description and Functional Definition [L.29.2.1; C.2.1.1.1; C.2.1.1.1.1]

As depicted in **Figure 2.1.1-2**, and delineated in **Table 2.1.1-6** and previously in **Section 2.1.1.1.1.1**, agencies will receive a VPNS solution that provides value added services, full-service scope, and functional capabilities.

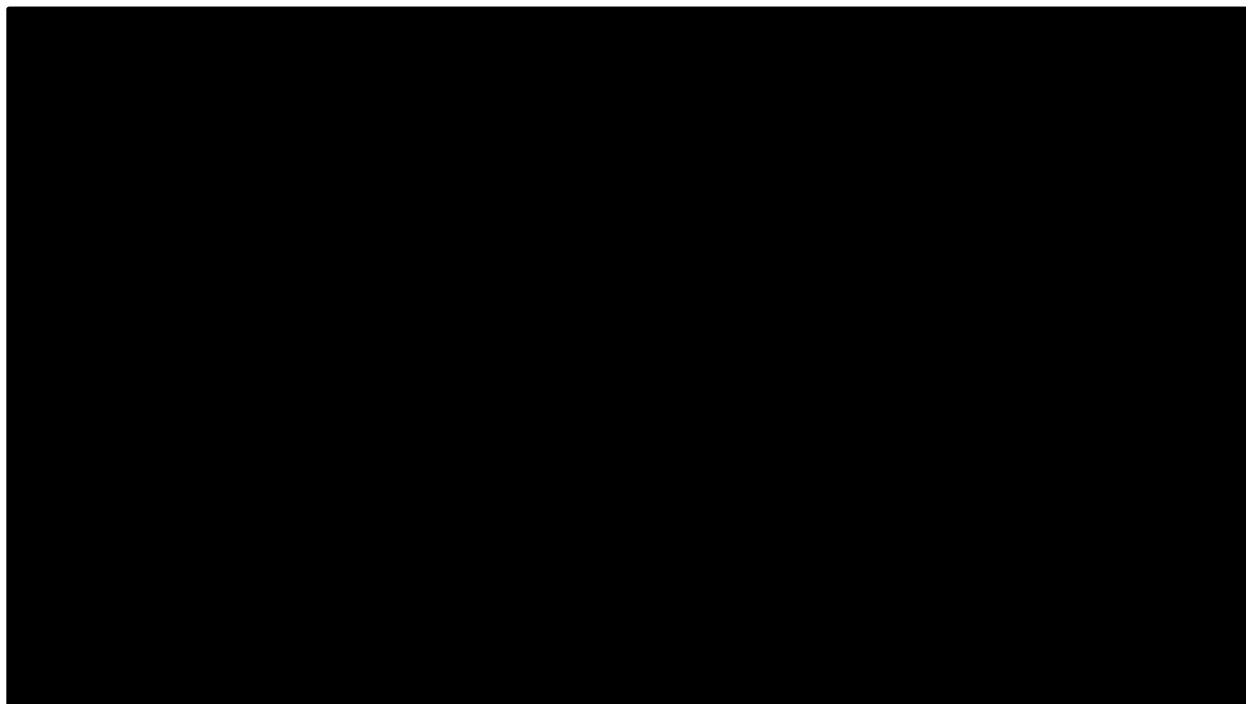


Figure 2.1.1-2. AT&T VPN with Value-Added Services.

Table 2.1.1-6. VPNS Service Scope and Functional Capabilities. Agencies will benefit from the AT&T VPNS architecture to provide highly secured, private, and robust transport services that can be adapted to their priorities and missions. Internal and external traffic will be identified, prioritized, and transported efficiently and reliably.

Solution Element	Description
Secure, reliable transport	[REDACTED]
Infrastructure and device ownership	[REDACTED]
Three basic VPNS solutions	[REDACTED]
Application optimization	[REDACTED]
Range of traffic	[REDACTED]
Proprietary technology	[REDACTED]

2.1.1.1.2.2 Standards [L.29.2.1; C.2.1.1.1.2]

AT&T will comply with all applicable standards listed in the RFP, as well as those referenced by the listed standards, as applicable.

2.1.1.1.2.3 Connectivity [L.29.2.1; C.2.1.1.1.3]

AT&T will comply with all connectivity instances listed in the RFP, as applicable.

2.1.1.1.2.4 Technical Capabilities [L.29.2.1; C.2.1.1.1.4]

As delineated in **Table 2.1.1-7**, and previously depicted in **Figure 2.1.1-2** and described in **Section 2.1.1.1.1.1**, agencies will receive a currently operational VPNS that meets all mandatory technical capabilities.

Table 2.1.1-7. VPNS Technical Capabilities. Agencies benefit from a broad feature set to route, provide security for and verify their private data to global users and locations.

#	Technical Capability		Description
1.	Routing	[REDACTED]	[REDACTED]
2.	Tunneling	[REDACTED]	[REDACTED]
3.	Encryption	[REDACTED]	[REDACTED]

[illegible]

As delineated in **Table 2.1.1-8**, and described previously in **Section 2.1.1.1.1.1**, agencies will receive a VPNS that meets or exceeds all mandatory features and optional features, as applicable. AT&T VPNS offers agencies the [REDACTED]

Device Type	Percentage of Respondents
Smartphone	95%
Tablet	85%
Smartwatch	70%
Smart TV	55%

Table 2.1.1-8. VPNS Features. Agencies receive an extensive set of VPNS features that meet or exceed requirements. The option to provide diversity in the design will allow agencies to develop the right level of reliability for critical locations and applications.

#	Feature		Description
RFP -Required Features			
1.	High availability options		
2.	Interworking services (optional)		
	Interfaces		
Additional Features			
	Switch diversity option		
	PoP diversity option		
	Any-to-any connections		
	Class of service		
	MD5 authentication		
	IPv4/IPv6 dual-stack support		
	Multicast support		
	Route group option		
	BFD		

2.1.1.1.2.6 Interfaces [L.29.2.1; C.2.1.1.3]

The AT&T VPNS is .

2.1.1.1.2.7 Performance Metrics [L.29.2.1; C.2.1.1.4]

The AT&T VPNS meets all KPIs listed in RFP Section C.2.1.1.4.

2.1.1.2 Ethernet Transport Service [L.29.2.1; M.2.1; C.2.1.2]

The AT&T ETS is the Layer 2 Service offer will connect customer agencies together at

[REDACTED]
[REDACTED]

[REDACTED]. Offering the same flexibility over long distances that are enjoyed in an agency's

LAN, AT&T ETS will provide scalable Ethernet (i.e., Bandwidth-On-Demand) [REDACTED]

[REDACTED].

AT&T ETS Experience/Accomplishments	
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]
—	[REDACTED]
	[REDACTED]

2.1.1.2.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.1.1.2.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

Blending the best of our comprehensive local and long-haul Ethernet services suites, the AT&T proposed solution for ETS will offer agencies a Metro Ethernet Forum (MEF) certified carrier-class Layer 2 VPN, which allows the connection of multiple sites in a single bridged domain over the AT&T managed MPLS network. ETS will provide point-to-point (E-LINE), point-to-rooted multipoint (E-LAN), and multipoint-to-multipoint (E-LAN) services. ETS will provide connectivity for/between LANs, Metropolitan Area Networks (MAN), and WANs at speeds of 10 Mbps, 100 Mbps, and 1 Gbps, and 10 Gbps with the capability to scale to 40 Gbps and 100 Gbps. Connection-oriented ETS will provide a desirable, low-risk migration path for agencies with PL and other legacy networks.

AT&T ETS is a carrier-grade service [REDACTED]

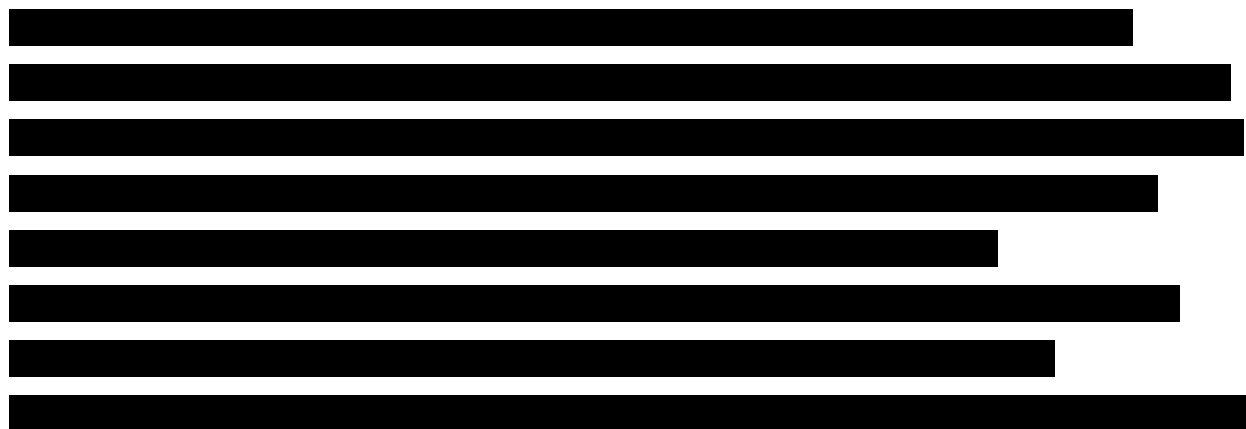
[REDACTED],

AT&T is able to offer point-to-point, point-to-multipoint, and multipoint-to-multipoint services with no geographical limitation, provided that Ethernet is available at the

[REDACTED]

[REDACTED]

[REDACTED]. The network ties together service instances of customer VPN into an



in **Figure 2.1.1-3** and **Table 2.1.1-9**.

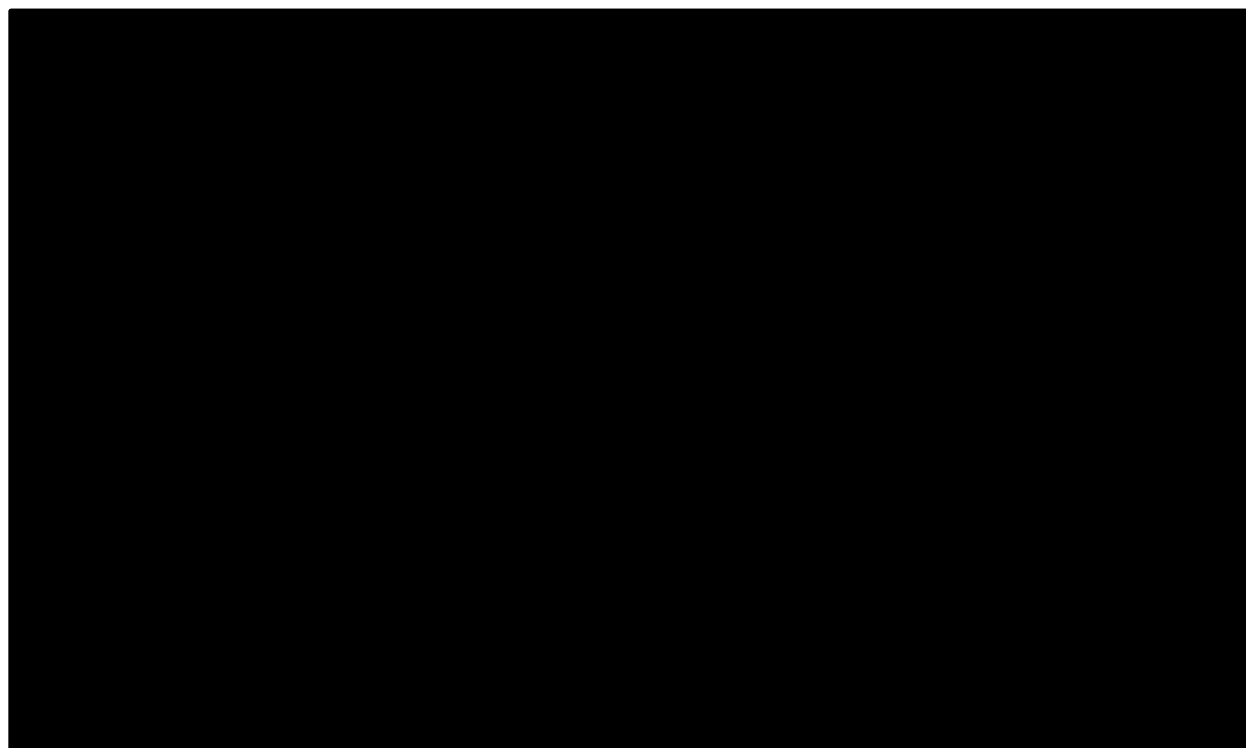






Figure 2.1.1-3. ETS Overview.

Table 2.1.1-9. ETS Overview Description. *ETS components are offered through MEF-certified carrier-class Layer 2 VPN, allowing connection of multiple sites in single bridged domain over the AT&T managed IP/MPLS network, providing point-to-point (E-LINE), point to multipoint (E-LAN) and multipoint to multipoint (E-LAN) services.*

Architectural Components	Description
Functional Components	
	
	

Architectural Components	Description
	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Technical Components	
Local access	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Port	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Ethernet Virtual Connection (EVC)	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
QoS	<ul style="list-style-type: none"> [REDACTED]
Operational Components	
Ethernet Private Line Service (EPLS)	<ul style="list-style-type: none"> [REDACTED]
Ethernet Virtual Private LAN Service (VPLS)	<ul style="list-style-type: none"> [REDACTED]
Ethernet virtual connections	<ul style="list-style-type: none"> [REDACTED]
Service level agreements	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Diverse access	<ul style="list-style-type: none"> [REDACTED]
Alternate serving switch	<ul style="list-style-type: none"> [REDACTED]
Business center	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
TDM emulation	<ul style="list-style-type: none"> [REDACTED]
Network Components	
Juniper MX480/980	<ul style="list-style-type: none"> [REDACTED]
MPLS core	<ul style="list-style-type: none"> [REDACTED]

2.1.1.2.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

As delineated in **Table 2.1.1-10**, our approach and architecture for ETS will deliver compliant, scalable, reliable, and resilient service.

Table 2.1.1-10. ETS QoS.

Compliance	
Demonstrated capability	
Scalability	
Speeds	
Network topologies	
Options	
Reliability	
AT&T backbone	
Resilience	
Backbone routers	
Backbone trunks	

2.1.1.2.1.3 Service Coverage (CBSA-Dependent) [L.29.2.1(C); M.2.1(3); C.1.3]

See **Section 1.3** for AT&T service coverage for ETS.

2.1.1.2.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.1.1.2.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

ETS has no service-specific requirements indicated in the RFP. Agencies will fully control their switching and routing as well as security, and will not share routing tables with AT&T.

2.1.1.2.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for ETS are protected from information breaches, unauthorized access and supply chain risks worldwide by The AT&T global security architecture. The AT&T service design and deployment is built upon continuous security risk management at operational, business process and systems levels.

2.1.1.2.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3)]

Table 2.1.1-11

Table 2.1.1-11. Approach to External Traffic Routing Requirements. Agencies will receive services that operate on a network that meets all external traffic routing requirements as described in the AT&T network architecture.

Requirement	Approach
Methodology for Identifying AT&T Participating Agency Traffic for Each Affected Service [M.2.1.4.c.i]	Section 1.4.3.1.
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 [M.2.1.4.c.ii]	Section 1.4.3.2.
Technical Approach to Notify DHS If Any Non-Participating Agency Traffic Will Be Redirected Through DHS EINSTEIN Enclaves [M.2.1.4.c.iii]	Section 1.4.3.3.
Control Mechanisms to Ensure the Identification and Redirection of Participating Agency Traffic Cannot Be Inadvertently or Maliciously By-Passed [M.2.1.4.c.iv]	Section 1.4.3.4.
Sensing and Control Mechanisms to Ensure the Redirection of Traffic is Failsafe [M.2.1.4.c.v]	Section 1.4.3.5.
Location of AT&T Certified Facilities [M.2.1.4.c.vi]	Section 1.4.3.6.
Availability of TS/SCI Cleared Personnel for “Smart-Hands” Service of DHS Supplied Equipment [M.2.1.4.c.vii]	Section 1.4.3.7.
Instrumentation to Measure Transport SLA KPIs [M.2.1.4.c.viii]	Section 1.4.3.8.

2.1.1.2.2 Technical Response for ETS [L.29.2.1; M.2.1]

2.1.1.2.2.1 Service Description and Functional Definition [L.29.2.1; C.2.1.2.1; C.2.1.2.1.1]

As described in **Table 2.1.1-12**, and previously in **Section 2.1.1.2.1.1**, agencies will benefit from an ETS solution that provides the full service scope and functional capabilities.

Table 2.1.1-12. ETS Service Scope and Functional Capabilities. Agencies will receive an ETS solution with demonstrated capability to meet service description and functional requirements. [REDACTED], depending on agency-specific requirements.

Solution Element	Description
[REDACTED]	[REDACTED]
Interconnection	[REDACTED]
Multiple service types	[REDACTED]
Connection types	[REDACTED]
Proprietary technology	[REDACTED]

2.1.1.2.2.2 Standards [L.29.2.1; C.2.1.2.1.2]

AT&T will comply with standards listed in the RFP, as well as those referenced by the listed standards, as applicable.

2.1.1.2.2.3 Connectivity [L.29.2.1; C.2.1.2.1.3]

AT&T will comply with connectivity instances listed in the RFP, as applicable.

2.1.1.2.2.4 Technical Capabilities [L.29.2.1; C.2.1.2.1.4]

As described in **Table 2.1.1-13**, and previously in **Section 2.1.1.2.1.1**, agencies will receive an ETS that meets all mandatory technical and optional technical capabilities, as applicable.

Table 2.1.1-13. ETS Technical Capabilities. Agencies will receive services that meet required technical capabilities, enabled by MEF-compliant, AT&T Labs-certified Ethernet network elements.

#	Technical Capability	[REDACTED]	Description
1.	Routing requirements	[REDACTED]	[REDACTED]
2.	Geographical coverage	[REDACTED]	[REDACTED]

#	Technical Capability		Description
3.	Ethernet UNI (User-to-Network-Interface)		
4.	EVCs		
5.	Delivery at the agency's SDP		
6.	Circuit emulation services for TDM services		
7.	Point-to-point, multipoint-to-multipoint, and point-to-multipoint EVCs		
8.	EVC multiplexing		
9.	Rate-limited throughput access links		
10.	Rate-limiting		
11.	Privacy and security		
12.	Physical interfaces		
13.	Supported traffic profiles		
14.	Performance parameters		
15.	Service frame delivery options		
16.	VLAN tag		

#	Technical Capability		Description
17.	Service multiplexing		
18.	Bundling		
19.	Security filters		
20.	Proactive performance monitoring (optional)		
21.	Maintenance functions		
22.	Network topologies		
23.	Geographical diversity		
24.	Bridging		
25.	Virtual connection sizes		
26.	Quality of service		
27.	Traffic reconfiguration		

2.1.1.2.2.5 Features [L.29.2.1; C.2.1.2.2]

The RFP indicates no features for ETS.

2.1.1.2.2.6 Interfaces [L.29.2.1; C.2.1.2.3]

The AT&T ETS is compatible with the interfaces referenced in RFP Section C.2.1.2.3, as applicable.

2.1.1.2.2.7 Performance Metrics [L.29.2.1; C.2.1.2.4]

2.1.2 Service Area: Voice Service [L.29.2.1; M.2.1; C.2.2]

AT&T proposes IP Voice Service (IPVS) as the mandatory voice services component.

2.1.2.1 Internet Protocol Voice Service [L.29.2.1; M.2.1; C.2.2.1]

The AT&T IP Voice Service (IPVS) will provide customer agencies with a

while minimizing disruptions in worker productivity.

2.1.2.1.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.1.2.1.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

The proposed AT&T IPVS will offer complete and robust communications services to agencies over a

The landscape of communications is changing. The IPVS infrastructure is quickly replacing the old circuit switched systems and currently provides IP-based voice services to both government and commercial customers.

requirements described in **Table 2.1.2-1** and shown in **Figure 2.1.2-1**.

Table 2.1.2-1. IPVS Overview Description. *IPVS components have been in use by federal and DoD agencies for over a decade.*

Architectural Components	Description
Functional Components	
IPVS network infrastructure	

Use or disclosure of data contained on this page is subject to the restriction on the title page of this document.

Architectural Components	Description
IP Border Elements (IPBE)	<ul style="list-style-type: none"> ■ [Redacted] ■ [Redacted]
IP/MPLS network	<ul style="list-style-type: none"> ■ [Redacted] ■ [Redacted]
Provider Edge (PE) and CE routers	<ul style="list-style-type: none"> ■ [Redacted] ■ [Redacted] ■ [Redacted]
VoIP Demarcation Unit (Demarc)	<ul style="list-style-type: none"> ■ [Redacted]
Customer gateways	<ul style="list-style-type: none"> ■ [Redacted]

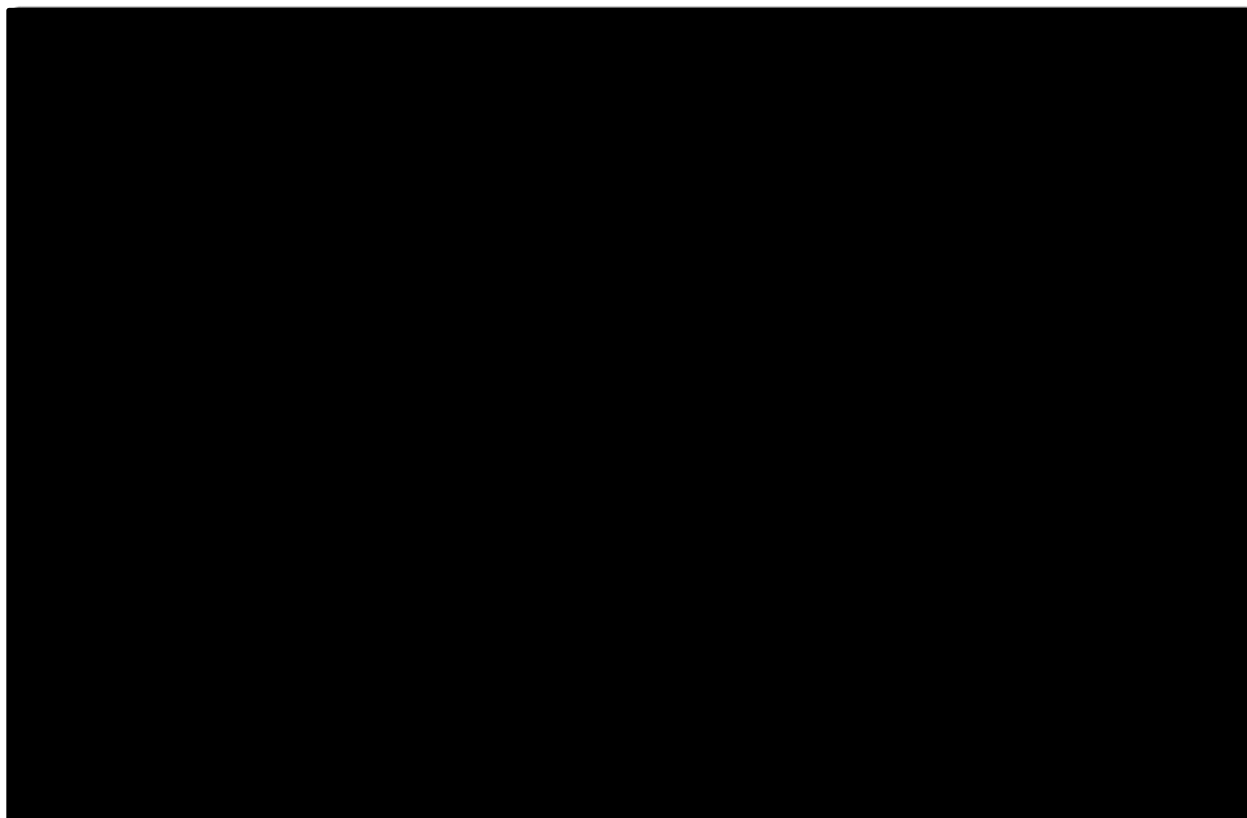


Figure 2.1.2-1. IPVS Overview.

2.1.2.1.1.2 Quality of Services [L.29.2.(B); M.2.1(2)]

As described in **Table 2.1.2-2**, our approach and architecture for delivering IPVS will deliver compliant, scalable, reliable, and resilient service.

Table 2.1.2-2. IPVS QoS. *IPVS is fully compliant, and provides the robust scalability, high reliability, and strong resilience sought by GSA and customer agencies.*

Architectural Components	Description
Compliance	
Demonstrated compliance	<ul style="list-style-type: none"> Section 2.1.2.1.2
Scalability	
Modular distributed architecture	<ul style="list-style-type: none">
IP/MPLS routes around failures	<ul style="list-style-type: none">
Reliability	
High availability service nodes	<ul style="list-style-type: none">
Service at IP location	<ul style="list-style-type: none">
Resilience	
Geo-redundant service nodes	<ul style="list-style-type: none">
Service at IP location	<ul style="list-style-type: none">

Architectural Components	Description
	<ul style="list-style-type: none"> ■ [REDACTED]
COOP support	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]

2.1.2.1.1.3 Service Coverage (CBSA-Dependent) [L.29.2.1(C); M.2.1(3); C.1.3]

See **Section 1.3** for AT&T service coverage for IPVS.

2.1.2.1.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.1.2.1.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

As described in **Table 2.1.2-3**, agencies will receive IP-based voice services with the best possible security using AT&T security standards, mechanisms, and procedures, coupled [REDACTED]

Table 2.1.2-3. [REDACTED] *AT&T is an industry leader in IP and IP application security* [REDACTED]

Capability	Description
Seven pillars of secure systems and networks	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
SIP authentication	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]
Denial of service protection	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]

Capability	Description
Intrusion detection and protection	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Invasion of privacy protection	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Proxy authentication for IPVS internal and external devices	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

2.1.2.1.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for IPVS will be protected from information breaches, unauthorized access, and supply chain risks worldwide by the AT&T global security architecture. The AT&T service design and deployment is built upon [REDACTED]

2.1.2.1.2 Technical Response for IPVS [L.29.2.1; M.2.1]

2.1.2.1.2.1 Service Description and Functional Definition [L.29.2.1; C.2.2.1.1; C.2.2.1.1.1]

As described in **Table 2.1.2-5**, and previously in **Section 2.1.2.1.1.1**, agencies will receive a solution that provides the full service, scope and functional capabilities.

Table 2.1.2-5. [REDACTED]. Agencies will receive service with established capability to meet service description and functional requirements.

Solution Element	Description
Telephone service	<ul style="list-style-type: none"> [REDACTED]

Solution Element	Description
Voice calls	<ul style="list-style-type: none"> Support voice calls initiated from on-net or off-net locations and connected to all on-net and off-net locations by direct dialing
Proprietary technology	<ul style="list-style-type: none"> Uses no proprietary technology for this service

2.1.2.1.2.2 Standards [L.29.2.1; C.2.2.1.1.2]

AT&T will comply with all standards listed in the RFP, as well as those referenced by the listed standards, as applicable.

2.1.2.1.2.3 Connectivity [L.29.2.1; C.2.2.1.1.3]

AT&T will comply with all connectivity instances listed in the RFP, as applicable.

2.1.2.1.2.4 Technical Capabilities [L.29.2.1; C.2.2.1.1.4]

As described in **Table 2.1.2-6**, and previously in **Section 2.1.2.1.1.1**, agencies will receive an established IPVS that meets all mandatory technical capabilities.

[REDACTED]. Agencies will receive IPVS [REDACTED]

Technical Capability	Description
Calling capability	[REDACTED]
Remote calling capability	[REDACTED]
Telephone usage capabilities	[REDACTED]
IPVS gateways	[REDACTED]

Technical Capability		Description
Station registration and mobility		<p>[REDACTED]</p> <p>[REDACTED]</p>
Agency firewall traversal		<p>[REDACTED]</p>
Service security architecture		<p>[REDACTED]</p>
Security practices and safeguards		<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
Emergency calling		<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
FCC local number portability support		<p>[REDACTED]</p>

2.1.2.1.2.5 Features [L.29.2.1; C.2.2.1.2]

As described in **Table 2.1.2-7**, and previously in **Section 2.1.2.1.1.1**, agencies will receive an established IPVS that meets or exceeds all mandatory features.

Table 2.1.2-7. [REDACTED]. Agencies will receive [REDACTED].

#	Feature		Description
1.	Voice mail box		<p>[REDACTED]</p> <p>[REDACTED]</p>

#	Feature		Description
			[REDACTED]
2.	Auto attendant		[REDACTED]
3.	Augmented 911/E911 IP PS/ALI		[REDACTED]
	Calling features (1-21)		[REDACTED]
	Telephony manager (administrator) (22)		[REDACTED]
	Telephony manager (subscriber) (23)		[REDACTED]
Additional Capabilities (available for an additional fee)			
4.	Site survivability		[REDACTED]

2.1.2.1.2.6 Interfaces [L.29.2.1; C.2.2.1.3]

The AT&T IPVS is compatible with the interfaces referenced in RFP Section C.2.2.1.3, as applicable.

2.1.2.1.2.7 Performance Metrics [L.29.2.1; C.2.2.1.4]

AT&Ts IPVS meets all KPIs referenced in RFP Section C.2.2.1.4.

2.1.2.1.2.8 Managed LAN Service (MLS) [C.2.2.1.5]

The AT&T MLS will provide agencies with on-premises LAN equipment that is configured to facilitate Voice over IP calling.

. As depicted in **Figure 2.1.2-2** and described in **Table 2.1.2-8**, agencies will receive a MLS solution that provides the full service, scope, and functional capabilities.

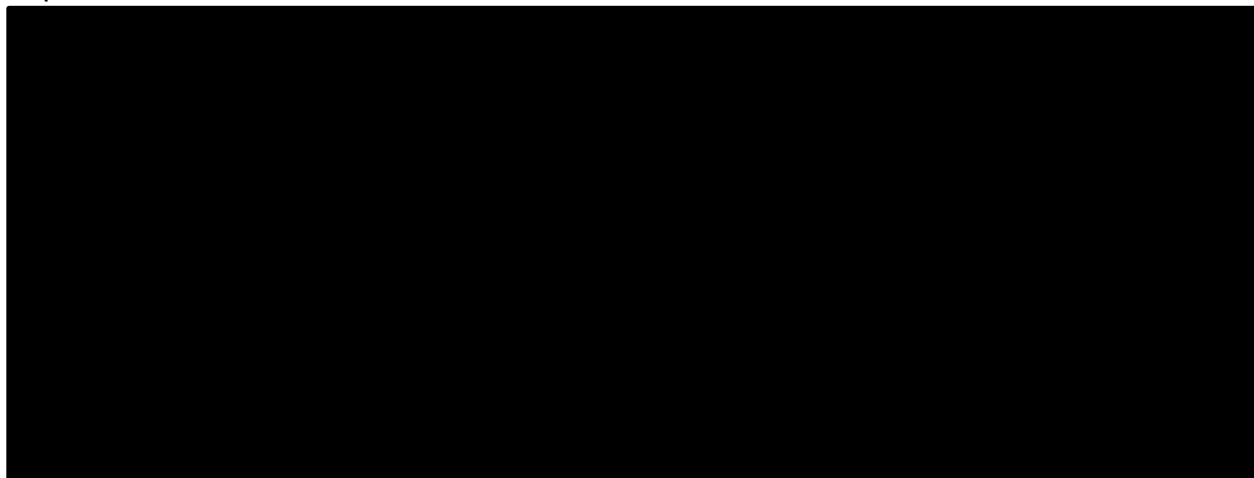


Figure 2.1.2-2. The Managed LAN Overview.

Table 2.1.2-8. MLS Scope and Functional Capabilities. Agencies will receive service with established capability

Solution Element	Description
MLAN equipment	
POE	
Systems maintenance	
Custom LAN buildout	

Solution Element	Description
	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
Proprietary technology	<ul style="list-style-type: none"> ■ Uses no proprietary technology.

As described in **Table 2.1.2-9**, agencies will receive a managed LAN that meets all mandatory technical capabilities.

Table 2.1.2-9. MLS Technical Capabilities. Agencies will receive [REDACTED]

#	Technical Capability		
1.	VoIP-LAN integration		<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
2.	Cabling limitation		<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
3.	Maintenance and upgrades		<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]
4.	Site expansion		<ul style="list-style-type: none"> ■ [REDACTED]
5.	WiFi capability		<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
6.	Data LAN support		<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]
7.	SIP registration and VoIP support		<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]

#	Technical Capability		
8.	Monitoring and management		<ul style="list-style-type: none">
9-11.	Trouble ticketing, notification, and escalation		<ul style="list-style-type: none">
	Custom LAN buildout		<ul style="list-style-type: none">

2.1.2.1.2.9 Session Initiation Protocol (SIP) Trunk Service [C.2.2.1.6]

As described in **Table 2.1.2-10**, agencies will receive a SIP solution that provides the full service, scope, and functional capabilities.

Table 2.1.2-10. SIP Scope and Functional Capabilities. Agencies will receive service with established capability that

Solution Element	Description
PBX interoperability	
IPVS network integration	
Proprietary technology	

2.1.2.1.2.9.1 Technical Capabilities [C.2.2.1.6.1]

As described in **Table 2.1.2-11**, agencies will receive SIP Trunk Service that meets all mandatory technical capabilities.

Table 2.1.2-11. SIP Technical Capabilities. Agencies will receive SIP Trunk Service that

Technical Capability	Description
SIP call routing	

2.1.2.1.2.9.2 Features [C.2.2.1.6.2]

As described in **Table 2.1.2-12**, and depicted previously in **Figure 2.1.2-1**, agencies receive established SIP Trunk Service that

Table 2.1.2-12. SIP Trunk Service Features. Agencies receive SIP Trunk Service that meets

Feature		How Delivered
Automatic call routing		
Bandwidth management		
Trunk bursting		
Number blocks		

2.1.2.2 Circuit Switched Voice Service [L.29.2.1; M.2.1; C.2.2.2]

AT&T Circuit Switched Voice Services (CSVS) supports voice calls, whether initiated from on-net or off-net locations, to be connected to all on-net and off-net locations by direct dialing throughout the U.S. CSVS encompasses both traditional local and long distance service, and enables users to call, or receive calls from, any phone in the U.S. or the world. CSVS connects to and interoperates with a broad range of equipment including single-line telephones, secure terminal equipment, conference room audio equipment, modems, and facsimile machines.

2.1.2.2.1 How AT&T Will Provide the Proposed Services and Features [L.29.2.1; M.2.1]

2.1.2.2.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

CSVS uses call switching equipment and circuit infrastructures to provide voice services in traditional interfaces such as POTS lines, T-1s, and ISDN trunks. CSVS supports all direct dialed voice calls throughout the U.S. regardless of whether initiated or terminated on the same or different networks (on-net and off-net respectively). CSVS operates over the public switched telephone network (PSTN) (wireline and wireless) in CONUS, OCONUS, and non-domestic locations.

[REDACTED]

[REDACTED]

[REDACTED] **Figure**

2.1.2.2-1 [REDACTED]

[REDACTED].

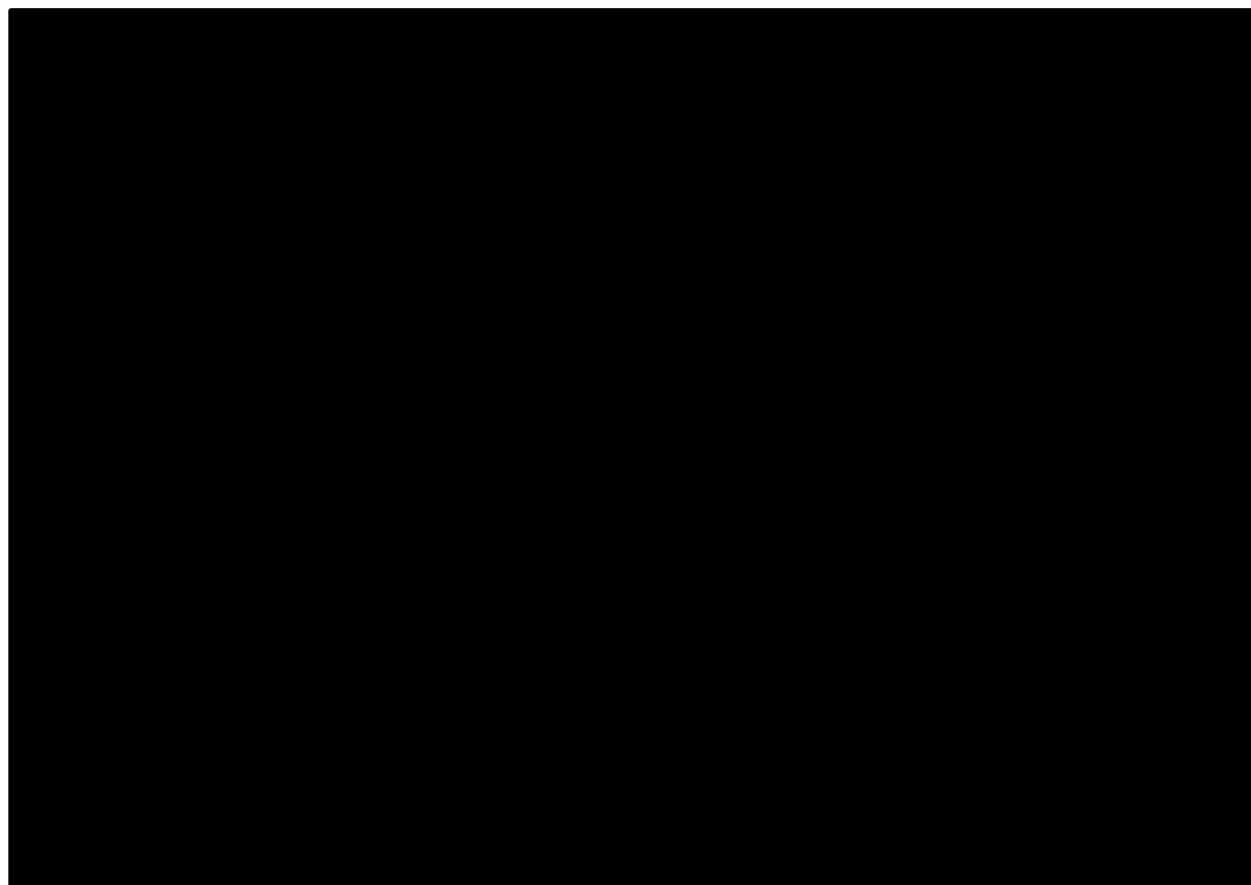


Figure 2.1.2.2-1. CSVS Overview. [REDACTED]

[REDACTED] **Table 2.1.2.2-1,** [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Table 2.1.2.2-1. CSVS Overview Description.

Architectural Components	Description
Functional Components	
Line	
CENTREX	
Trunk	
Voicemail	
CO/Switch	
Technical Components	
Numbering	
LNP	
Emergency Services (Dial 911)	
PSTN	
Interconnect Agreements	
Operational Components	
AT&T Voice NOC	
SS7	
Network Components	
5ESS and DMS Switches	
SS7 Signaling and interconnect Network	
Serving Wire Center (SWC)	
Access Circuits	

2.1.2.2.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

[REDACTED]

Table 2.1.2.2-2.

Table 2.1.2.2-2. CSVS Quality of Service.

Architectural Components	Description
Compliance	
Service & Functional Req'ts	■ [REDACTED] Section 2.1.2.2.2.1
Standards	■ [REDACTED] 2.1.2.2.2.2
Connectivity	■ [REDACTED] Section 2.1.2.2.2.3
Technical Capabilities	■ [REDACTED] Section 2.1.2.2.2.4
Features	■ [REDACTED] Section 2.1.2.2.2.5
Interfaces	■ [REDACTED] Section 2.1.2.2.2.6
Performance Metrics	■ [REDACTED] Section 2.1.2.2.2.7
Scalability	
T-Carrier Delivery	■ [REDACTED]
Reliability	
NEBS Systems Architecture	■ [REDACTED]
SS7 Five-Nines	■ [REDACTED]
Resilience	
Single Circuit Service	■ [REDACTED]

[REDACTED]

See **Section 1.3** for AT&T service coverage for CSVS.

2.1.2.2.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.1.2.2.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7]

[REDACTED]

[REDACTED]

Table 2.1.2.2-3

Table 2.1.2.2-3. CSVS Service-Specific Security Capabilities.

Capability	Description
PSTN Based Service	

2.1.2.2.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

Section 1.4

2.1.2.2.2 Technical Response for CSVS [L.29.2.1; M.2.1]

2.1.2.2.2.1 Service Description and Functional Definition [L.29.2.1; C.2.2.2.1; C.2.2.2.1.1]

Table 2.1.2.2-4 and depicted in Figure 2.1.2.2-1.

Table 2.1.2.2-4. CSVS Service Scope and Functional Capabilities.

Solution Element	Description
Voice Calls	
Equipment	
PSTN	

2.1.2.2.2.2 Standards [L.29.2.1; C.2.2.2.1.2; C.1.8.4]

AT&T will comply with all voice service industry standards.

2.1.2.2.2.3 Connectivity [L.29.2.1; C.2.2.2.1.3]

AT&T will comply with all connectivity instances listed in the RFP, as applicable.

2.1.2.2.2.4 Technical Capabilities [L.29.2.1; C.2.2.2.1.4]

Table 2.1.2.2-5 and depicted in Figure 2.1.2-1.

Table 2.1.2.2-5. CSVS Technical Capabilities.

Technical Capability		How Delivered
Numbering Plan and Number Assignments		<ul style="list-style-type: none">
Network Intercept		<ul style="list-style-type: none">
User-to-User Signaling (Optional)		<ul style="list-style-type: none">
Voice Quality		<ul style="list-style-type: none">
Emergency Service		<ul style="list-style-type: none">
Basic Subscriber Line		<ul style="list-style-type: none">
ISDN PRI		<ul style="list-style-type: none">
ISDN BRI		<ul style="list-style-type: none">
Additional Line Types		<ul style="list-style-type: none">

Technical Capability		How Delivered

2.1.2.2.2.5 Features [L.29.2.1; C.2.2.2.2]

Table 2.1.2.2-6

Figure 2.1.2.2-1.

Table 2.1.2.2-6. CSVS Features.

Feature		How Delivered
Agency-Recorded Message Announcements		
Authorization Codes/Calling Cards (optional)		
Caller Identification (ID)		
Call Screening for Users		
Class of Service (CoS) and Restrictions		

Feature		How Delivered
Code Block (optional)		
Customized Network Announcement Intercept Scripts (optional)		
Internal Agency Accounting Code (optional)		
Directory Assistance		
Suppression of Calling Number Delivery		
Voice Mail Box		
Basic Subscriber Line: Multi Appearance Directory Number (optional)		
ISDN PRI: Backup of Shared-D Channel (optional)		
ISDN BRI: Multi Appearance		

Feature		How Delivered
Directory Number (optional)		<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
MLPP (optional)		<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Additional Features		
		<ul style="list-style-type: none"> [REDACTED]

2.1.2.2.2.6 Interfaces [L.29.2.1; C.2.2.2.3]

[REDACTED]

[REDACTED].

2.1.2.2.2.7 Performance Metrics [L.29.2.1; C.2.2.2.4; G.8.2]

[REDACTED]

[REDACTED].

2.1.3 .Service Area: Managed Service [C.2.8]

2.1.3.1 Managed Network Service [L.29.2.1; M.2.1; C.2.8.1]

Agencies will receive a MNS that provides a broad service portfolio, comprehensive service design, and customized solutions that match mission requirements and maintenance in a highly secured environment.

AT&T MNS Experience
<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

2.1.3.1.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.1.3.1.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

MNS will provide a broad service portfolio, comprehensive service design, and implementation, enabling agencies to quickly deploy a customized solution to match mission requirements and maintenance needs. MNS services will meet or exceed government requirements by providing an established customer deployed MNS. AT&T subject matter specialists will bring the experience and talent to meet agencies' unique

requirements as specified in TOs. AT&T has a long history of providing custom managed services, [REDACTED]

[REDACTED] Tables 2.1.3-1 and 2.1.3-2, [REDACTED] Figures 2.1.3-1 and 2.1.3-2, [REDACTED].

Table 2.1.3-1. MNS Overview Description. [REDACTED]

Architectural Components	Description
Functional Components	
Global client support centers	[REDACTED]
Architectural validation	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Event management	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Incident management	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Performance management	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Technical Components	
Resources	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

Architectural Components	Description
Design and engineering	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Implementation	<ul style="list-style-type: none"> [REDACTED]
Operational Components	
Processes	<ul style="list-style-type: none"> [REDACTED]
Operations	<ul style="list-style-type: none"> [REDACTED]
Life cycle management	<ul style="list-style-type: none"> [REDACTED]
Network Components	
Devices	<ul style="list-style-type: none"> [REDACTED]

Table 2.1.3-2. MNS Overall Architectural Approach.

Capability	Description
Project planning	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Requirements definition	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Preliminary design document	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Design certification	<ul style="list-style-type: none"> [REDACTED]
Site survey	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Site preparation	<ul style="list-style-type: none"> [REDACTED] [REDACTED]

Capability	Description
Implementation and installation	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Test and acceptance	<ul style="list-style-type: none"> [REDACTED]
Life cycle management	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]

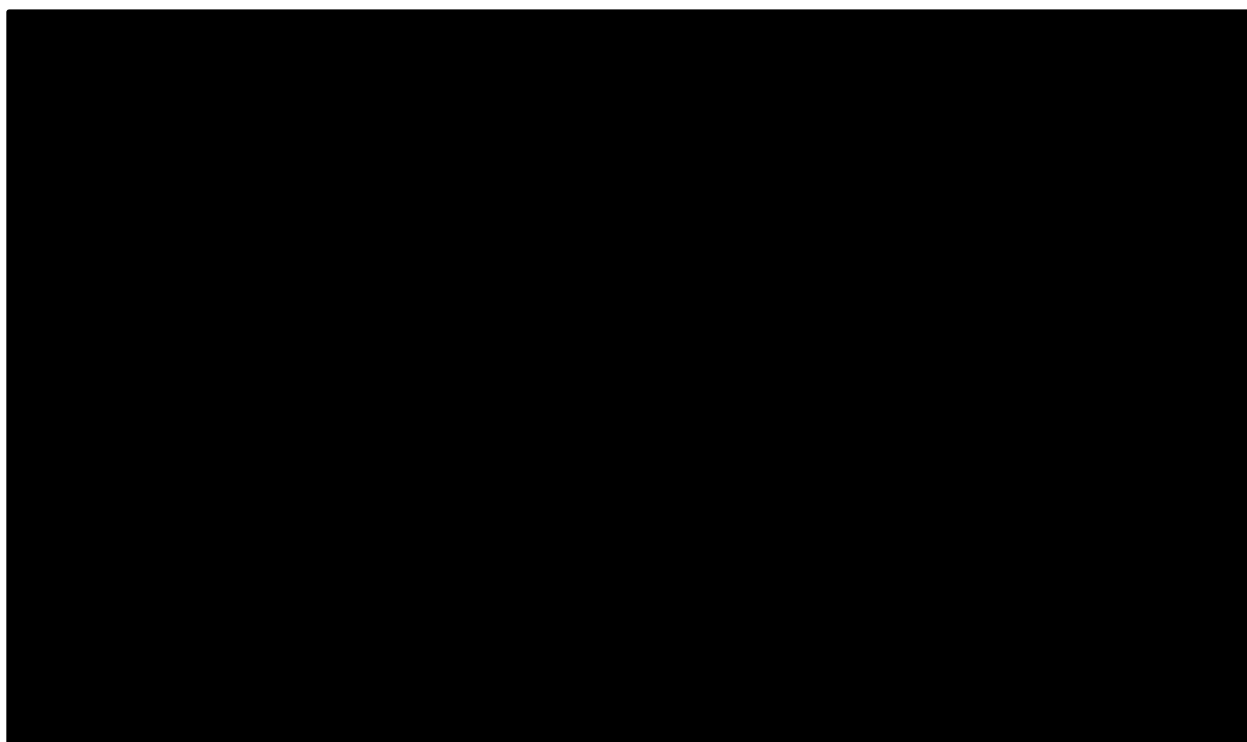


Figure 2.1.3-1. MNS Overview.

The AT&T management systems will provide

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Figure 2.1.3-2. AT&T Five-Phased MNS Approach.



2.1.3.1.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

As described in **Table 2.1.3-3**, our approach and architecture for delivering MNS will deliver compliant, scalable, reliable, and resilient service.

Table 2.1.3-3. MNS QoS. MNS is fully compliant, and provides the robust scalability, high reliability, and strong resilience sought by GSA and customer agencies.

Architectural Components	Description
Compliance	
Demonstrated compliance	<ul style="list-style-type: none"> [REDACTED]
Scalability	
Modular management systems architecture	<ul style="list-style-type: none"> [REDACTED]
Reliability	
Redundant system components	<ul style="list-style-type: none"> [REDACTED]
Resilience	
Asset and configuration management system	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Change management system	<ul style="list-style-type: none"> [REDACTED]
Deployment flexibility	<ul style="list-style-type: none"> [REDACTED] [REDACTED]

2.1.3.1.1.3 [REDACTED]

See **Section 1.3** for AT&T service coverage for MNS.

2.1.3.1.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.1.3.1.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

MNS security related capabilities are indicated in RFP Section C.2.8.1.1.4, and are addressed in proposal **Section 2.1.3.1.2.4**. **Table 2.1.3-4** delineates additional service-specific security capabilities delivered to customer agencies.

Table 2.1.3-4. MNS Service-Specific Security Capabilities. Agencies will receive highly secured services based on our overall architecture and service-specific capabilities.

Capability	Description
Secured MNS	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]

Capability	Description
Secured access and communications	
Modem and POTS line and wireless for OOB management	

2.1.3.1.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for MNS are protected from information breaches, unauthorized access and supply chain risks

2.1.3.1.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3)]

Our proposed architecture will meet all external traffic routing requirements applicable to MNS. **Table 2.1.3-5** provides detailed references to our approach.

Table 2.1.3-5. Approach to External Traffic Routing Requirements. Agencies receive services that operate on a network that meets all external traffic routing requirements as described in AT&T network architecture.

Requirement	Compliance Description
Methodology for Identifying AT&T Participating Agency Traffic for Each Affected Service [M.2.1.4.c.i]	Section 1.4.3.1.
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 [M.2.1.4.c.ii]	Section 1.4.3.2.
Technical Approach to Notify DHS If Any Non-Participating Agency Traffic Will Be Redirected Through DHS EINSTEIN Enclaves [M.2.1.4.c.iii]	Section 1.4.3.3.
Control Mechanisms to Ensure the Identification and Redirection of Participating Agency Traffic Cannot Be Inadvertently or Maliciously By-Passed [M.2.1.4.c.iv]	Section 1.4.3.4.
Sensing and Control Mechanisms to Ensure the Redirection of Traffic is Failsafe [M.2.1.4.c.v]	Section 1.4.3.5.
Location of AT&T Certified Facilities [M.2.1.4.c.vi]	Section 1.4.3.6.
Availability of TS/SCI Cleared Personnel for "Smart-Hands" Service of DHS Supplied Equipment [M.2.1.4.c.vii]	Section 1.4.3.7.

Requirement	Compliance Description
Instrumentation to Measure Transport SLA KPIs [M.2.1.4.c.viii]	Section 1.4.3.8.

2.1.3.1.2 Technical Response for MNS [L.29.2.1; M.2.1]

2.1.3.1.2.1 Service Description and Functional Definition [L.29.2.1; C.2.8.1.1; C.2.8.1.1.1]

Agencies will receive a solution that provides full service, scope, and functional capabilities, as described in **Table 2.1.3-6**, and described previously in **Section 2.1.3.1.1.1**.

Table 2.1.3-6. MNS Approach. *Experienced people, established processes, advanced tools, and client advocates will deliver outstanding network performance to agencies.*

Solution Element	Description
Capabilities provided	
Expert technical professionals	
Established program management, implementation, and help management processes	
Expert management systems and tools	
High-touch client servicing modeling	
Proprietary technology	

2.1.3.1.2.2 Standards [L.29.2.1; C.2.8.1.1.2]

MNS will support all EIS access and transport services and will be configured to meet the specific stands and requirements identified in a TO.

2.1.3.1.2.3 Connectivity [L.29.2.1; C.2.8.1.1.3]

MNS will work with underlying EIS offerings and provide seamless connectivity to agency network locations.

2.1.3.1.2.4 Technical Capabilities [L.29.2.1; C.2.8.1.1.4; C.2.8.1.1.4.1; C.2.8.1.1.4.2]

As illustrated in **Figure 2.1.3-1**, agencies will receive MNS Design and Engineering Services (DES), and Implementation, Management, and Maintenance (IMM) services, which meet all mandatory technical capabilities

. All proposed technical capabilities are described in **Table 2.1.3-7**, and described previously in **Section 2.1.3.1.1.1**.

Table 2.1.3-7. MNS Technical Capabilities. Agencies will receive service that meets required technical capabilities.

#	Technical Capability		Description
Design and Engineering Services (DES) [C.2.8.1.1.4.1]			
1.	Identify components		
2.	Identify network requirements		
3.	Project management		
Implementation, Management, and Maintenance (IMM) [C.2.8.1.1.4.2]			
1)	Comprehensive solutions		

#	Technical Capability		Description
2)	Hardware, firmware and related software supply and management		
3)	Monitor performance		
4).	Manage, proactively monitor, and report		
5)	SNMP data feeds		
6)	Manage network configuration		
7)	IP address management		
8)	Monitor and control access to equipment		
9)	Availability of recent configurations		
10)	Hardware and software upgrades, updates, patch deployments and bug fixes		
11)	Preventative and corrective maintenance		
12)	Problem detection, alert response, and reporting		
13)	Real or near-time access		
14)	Inventory tracking tools		
15)	Secure access to information		

2.1.3.1.2.5 Features [L.29.2.1; C.2.8.1.2]

Agencies will receive an established MNS that meets all mandatory features. All proposed features are described in **Table 2.1.3-8**, and described previously in **Section 2.1.3.1.1.1**.

Table 2.1.3-8. MNS Features. *Agencies will receive service that meets the required set of features.*

#	Feature		Description
1)	GFP maintenance		
2)	Network operations center and Security operations center		
3)	Network testing		
4)	Traffic aggregation service (DHS only)		

2.1.3.1.2.6 Interfaces [L.29.2.1; C.2.8.1.2; C.2.8.1.3]

The AT&T MNS is compatible with interfaces in RFP Section C.2.8.1.3, as applicable.

2.1.3.1.2.7 Performance Metrics [L.29.2.1; C.2.8.1.4]

The AT&T MNS meets all KPIs in RFP Section C.2.8.2.4.

2.1.4 Service Area: Access Arrangements [C.1.8.1]

2.1.4.1 Access Arrangements [L.29.2.1; M.2.1; C.2.9]

Agencies will receive fully compliant

that will deliver connectivity to all services, and offer service diversity for high availability using various legacy and emerging technologies.

AT&T Proven Access Arrangements Capabilities

2.1.4.1.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.1.4.1.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

The AT&T ever-expanding portfolio of access products and services will offer GSA customers scalable network infrastructure, pricing certainty, guaranteed availability, and high-quality service. Using AT&T access products and services facilitates smooth network expansion and evolution, and helps GSA to bring new value-added products to customer agencies faster than ever before.

GSA and its customer agencies will benefit from our experienced position as a current Networx Universal and Enterprise prime contractor, in which we provide the full range of legacy and emerging technologies to support current and evolving mission requirements. AT&T is a premier access provider with presence in more than [REDACTED]. As such, AT&T will provide GSA with a robust set of data and voice access alternatives. The AT&T proposed architecture and services will meet EIS service requirements as shown in **Table 2.1.4-1** and **Figure 2.1.4-1**.

Table 2.1.4-1. AA Overview Description. AA components will be provided by [REDACTED]

Architectural Components	Description
Functional Components	
Ethernet access network	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
Mobility core 4G/LTE network	[REDACTED]
	[REDACTED]
	[REDACTED]
Optical access network	[REDACTED]
	[REDACTED]
	[REDACTED]

Architectural Components	Description
Point-to-point microwave access links	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
TDM access network	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Technical Components	
Ethernet access network	<ul style="list-style-type: none"> [REDACTED]
Mobility core 4G/LTE network	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Optical access network	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Point-to-point microwave access links	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
TDM access network	<ul style="list-style-type: none"> [REDACTED]
Operational Components	
Business Support System (BSS)	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Engineering/design overall	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Network Components	
Access infrastructure	<ul style="list-style-type: none"> [REDACTED]

AT&T Flexibility: Our robust portfolio of AA will provide GSA with connectivity at agency-located SDPs to the AT&T PoPs. The wide range of line speeds and reliability options offered by AT&T will allow agency users to satisfy their diverse needs to access contractor networks. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

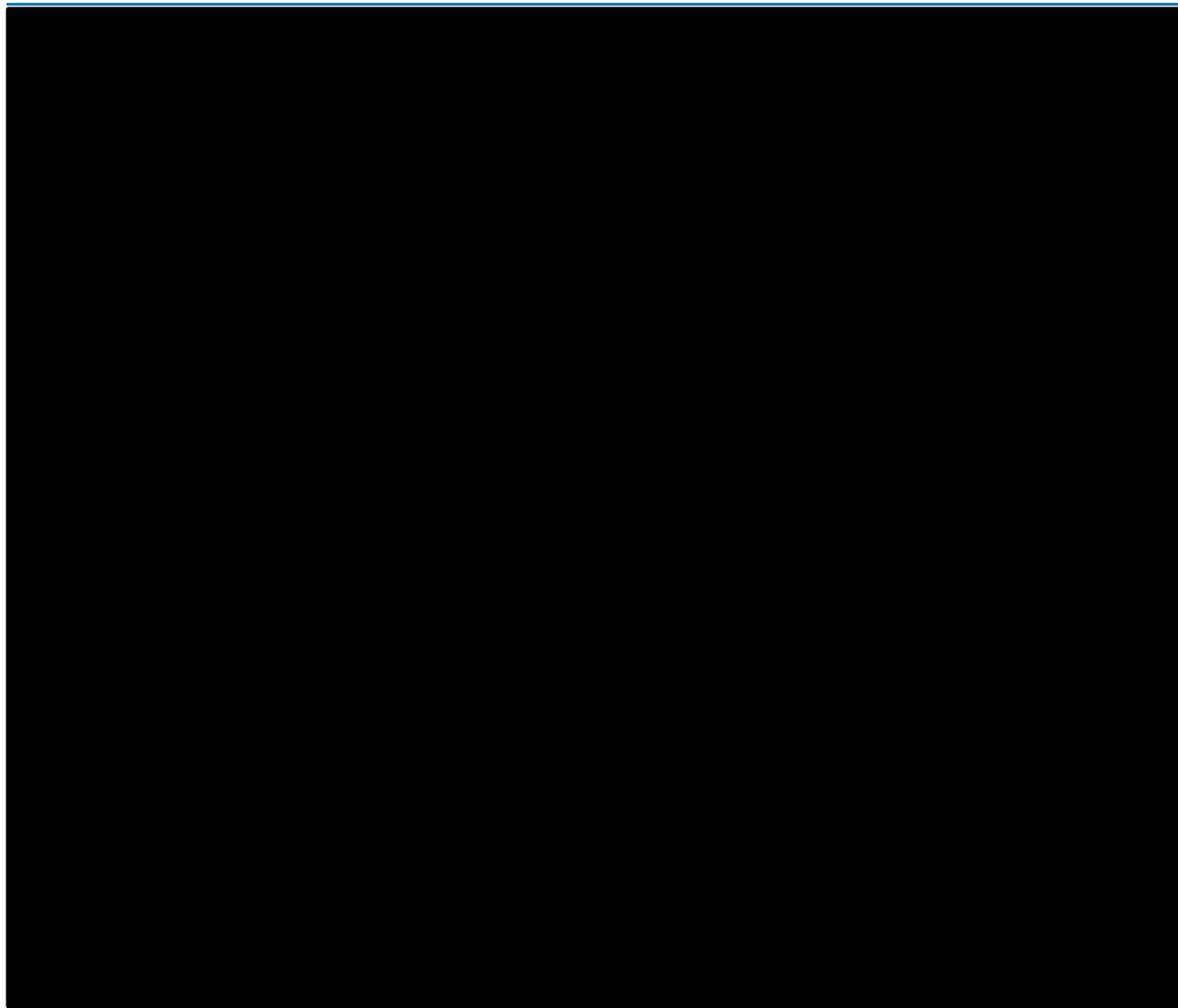


Figure 2.1.4-1. AA Overview.

2.1.4.1.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our approach and architecture for delivering AA delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.1.4-2**.

Table 2.1.4-2. AA QoS. AA is fully compliant, and provides the robust scalability, high reliability, and strong resilience sought by GSA and customer agencies. Service quality

Architectural Components	Description
Compliance	
Demonstrated capability	<div>■ [Redacted]</div> <div>Section 2.1.4.1.2 [Redacted]</div>

Architectural Components	Description
Scalability	
Speeds	■ [REDACTED]
AT&T network coverage	■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
Reliability	
Policies and programs	■ [REDACTED] ■ [REDACTED]
Resilience	
No single point of failure (core)	■ [REDACTED]

2.1.4.1.1.3 [REDACTED]

See **Section 1.3** for AT&T domestic coverage for AA. Mandatory wireline AA CLINs are provided at all NSCs within a proposed [REDACTED] as contained in the Traffic Model. OC-3 wireline access CLIN is provided at all NSCs within the proposed [REDACTED] when OC-3 is specified for the NSC in the Traffic Model. For NSCs within the proposed [REDACTED] that have Ethernet access CLINs associated with the Traffic Model, the mandatory Ethernet AA CLINs and incremental Ethernet AA CLINs associated with the Traffic Model are provided. Additionally, AA CLINs for NSCs beyond those contained in the Traffic Model have been provided. [REDACTED]

[REDACTED] Section 1.3.

2.1.4.1.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.1.4.1.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

While AA has no service-specific requirements indicated in the RFP, **Table 2.1.4-3** delineates additional service-specific security capabilities delivered to agencies.

Table 2.1.4-3. AA Service-Specific Security Capabilities. Agencies will receive highly secured services based on our overall architecture and service-specific capabilities. These capabilities are provided [REDACTED]

Capability	Description
AT&T security operations	■ [REDACTED]
Security experience	■ [REDACTED]
Security control	■ [REDACTED]

2.1.4.1.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.1.4.1.2 Technical Response for AA [L.29.2.1; M.2.1]

2.1.4.1.2.1 Service Description and Functional Definition [L.29.2.1; C.2.9.1; C.2.9.1.1]

Agencies will receive a solution that provides full service, scope, and functional capabilities, as described in **Table 2.1.4-5**, and described previously in **Section 2.1.4.1.1.1**.

Table 2.1.4-5. AA Service Scope and Functional Capabilities.

Solution Element	Description
Applications support	[REDACTED]
Special construction	[REDACTED]
Order fulfillment support	[REDACTED]
Proprietary technology	[REDACTED]

2.1.4.1.2.2 Standards [L.29.2.1; C.2.9.1.2]

AT&T will comply with all standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.1.4.1.2.3 Connectivity [L.29.2.1; C.2.9.1.3]

AT&T will comply with all connectivity instances listed in the RFP as applicable.

2.1.4.1.2.4 Technical Capabilities [L.29.2.1; C.2.9.1.4]

Agencies will receive established AA that meets all mandatory technical capabilities, [REDACTED]. All proposed technical capabilities are described in **Table 2.1.4-6**, and described previously in **Section 2.1.4.1.1.1**.

Table 2.1.4-6. AA Technical Capabilities. Agencies will receive service that meets required technical capabilities. All of these capabilities are provided via layer 1 TDM and layer 2 Ethernet network elements and supporting operational support systems.

#	Technical Capability		How Delivered
1.	Integrated access	[REDACTED]	[REDACTED]
2.	Transparency	[REDACTED]	[REDACTED]
1.	T1	[REDACTED]	[REDACTED]
2.	ISDN PRI	[REDACTED]	[REDACTED]
3.	ISDN BRI	[REDACTED]	[REDACTED]
4.	T3	[REDACTED]	[REDACTED]
5.	E1	[REDACTED]	[REDACTED]
6.	E3	[REDACTED]	[REDACTED]
7.	SONET OC-3	[REDACTED]	[REDACTED]
8.	SONET OC-12	[REDACTED]	[REDACTED]
9.	SONET OC-48	[REDACTED]	[REDACTED]
10.	SONET OC-192	[REDACTED]	[REDACTED]
11.	SONET 768 (optional)	[REDACTED]	[REDACTED]
12.	Analog line (4 KHz) (optional)	[REDACTED]	[REDACTED]

#	Technical Capability		How Delivered
13.	DS0		
14.	Subrate DS0 (optional)		
15.	Optical wavelength		
16.	Dark fiber (optional)		
17.	DSL access arrangements		
18.	Ethernet access arrangements		
19.	Cable high-speed (optional)		
20.	FTTP (optional)		
21.	Wireless access arrangements		

2.1.4.1.2.5 Features/Access Diversity and Avoidance [L.29.2.1; C.2.9.2]

Customer agencies will receive established AA that meets all mandatory features. All proposed features are described in **Table 2.1.4-7**, and described previously in **Section 2.1.4.1.1.1**.

2.1.4.1.2.6 Interfaces [L.29.2.1; C.2.9.3]

The AT&T proposed approach to AA is compatible with interfaces in RFP Section C.2.9.3, as applicable.

Table 2.1.4-7. AA Features. *Agencies will Receive Service that meets the Required Set of Features. Our proposed diversity and avoidance features will provide higher availability for critical agency sites.*

#	Feature		Description
RFP Required Features			

[illegible]

2.1.4.1.2.7 Performance Metrics [L.29.2.1]

The RFP indicates no performance metrics for AA.

2.1.5 Section 508 Requirements [C.4]

In accordance with the Americans with Disabilities Act (ADA) and government stipulations, AT&T EIS services are provided in a Section 508-compliant format in order to support a wide range of users with disabilities to access agency resources without the need for custom solutions.

2.1.5.1 Background [C.4.1]

As a provider of services similar to EIS under Networx and other federal contracts for over 20 years, AT&T operates with full awareness of the legislative and

regulatory background and requirements of Section 508 of the Rehabilitation Act of 1973.

To make our solutions accessible to the widest possible population of users with disabilities, AT&T follows a comprehensive accessibility testing approach that includes automated testing using state-of-the-art toolsets, manual testing against the leading industry practices in our Corporate Guide to Accessibility Checklist, and functional testing using assistive technology tools, such as (1) Jaws screen reader, (2) Dragon Naturally Speaking speech input software, and (3) Zoomtext magnifier software. To demonstrate compliance with Section 508 standards, AT&T will post to our web site within 30 days of Notice to Proceed the applicable Voluntary Product Accessibility Template (VPAT) for each offered EIS service in RFP Section C.4.4.

Our Section 508 and Corporate Accessibility Technology Organization accessibility experts collaborate with leading third-party accessibility vendors to evaluate our EIS services and develop the VPATs. We will build upon our experience developing the Networx VPATs, whose compliance was verified by independent audit.

Figure 2.1.5-1 illustrates the AT&T Section 508 Compliance Implementation Methodology for fulfilling the RFP Section C.4 requirements. Our lifecycle for developing products and Electronic and Information Technology (EIT) includes steps for systematically building in Section 508 compliance using leading industry-recognized accessibility practices, testing tools, and methodologies.

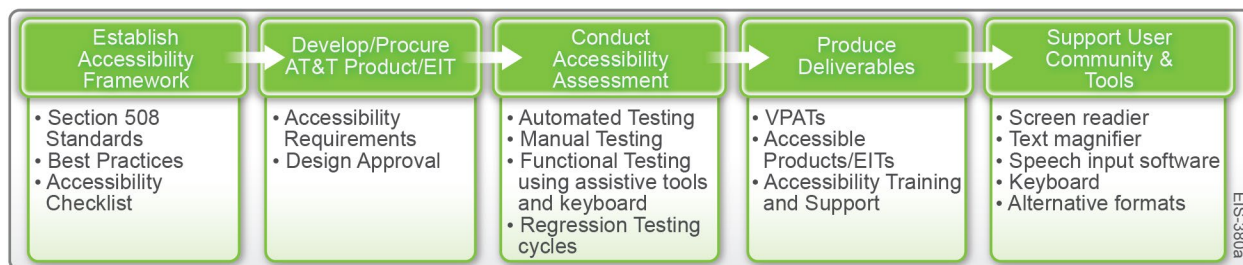


Figure 2.1.5-1. AT&T Section 508 Compliance Implementation Methodology. *To prevent accessibility delays and rework, our process assigns a trained accessibility solution engineer at the start of each project and builds 508 compliance into the system at each stage of development.*

2.1.5.2 Voluntary Product Accessibility Template [C.4.2]

AT&T will post the Voluntary Product Accessibility Template (VPAT) for each service identified in RFP Section C.4.4 to our web site within 30 days after NTP, and update the VPAT as needed, to demonstrate these offerings comply with Section 508 standards.

2.1.5.3 Section 508 Applicability to Technical Requirements [C.4.3; C.2]

AT&T EIS services will adhere to applicable RFP Section C.4.4 requirements concerning Section 508 accessibility, or we will provide equivalent facilitation.

Section 2.1.5.3 describes how we will address the requirements. For EIT products that are less than fully compliant with Section 508, AT&T will specify any standard that is not met, describe the non-compliance, and indicate the equivalent facilitation in the VPAT.

2.1.5.4 Section 508 Provisions Applicable to Technical Requirements [C.4.4]

For each EIS service, AT&T will fulfill the appropriate Section 508 technical and functional requirement as identified in RFP Section C.4.4. **Table 2.1.5-1** describes our approach for each type of product.

Table 2.1.5-1. How AT&T Fulfills Section 508 Subparts B, C, and D. *The AT&T approach to fulfilling Section 508 requirements applies to all offered product types and EIS services.*

§	Section 508 Requirements Citations	Compliance Description
§ 1194.21	Software applications and operating systems	<ul style="list-style-type: none"> Will deliver accessible software applications, web-based applications, and telecommunications products to users with disabilities who require assistive technologies, or provide equivalent facilitation. Whether developed in house or procured from a third-party vendor, AT&T accessibility engineers and third-party vendor specialists will assess and document compliance level in the corresponding VPAT sections.
§ 1194.22	Web-based intranet and Internet information and applications	
§ 1194.23	Telecommunications products	
§ 1194.31	Functional performance criteria	<ul style="list-style-type: none"> Will support the functional performance criteria as specified in RFP Section C.4.4. Whether developed in house or procured from a third-party vendor, the solutions will support assistive technologies used by individuals with disabilities or will provide equivalent facilitation.
§ 1194.41	Information, documentation, and support	<ul style="list-style-type: none"> Will provide alternative documentation formats to users free of charge on request. AT&T will also provide an overview of the product's accessibility features, optimal assistive technology configurations, means of requesting alternate formats, and known accessibility issues with the product.

2.1.5.5 Section 508 Provisions Applicable to Reporting and Training [C.4.5]

When delivering government information reports via the Internet, email, or telephone as required in RFP Section G.9, AT&T will support assistive technologies used by individuals with disabilities or will provide equivalent facilitation. Our reports will meet applicable Section 508 Standards in Subparts B, C, and D as explained in

Sections 2.1.5.2 and 2.1.5.3. When delivering government training via meetings and briefings, classroom, and seminars as required in RFP Section G.10, AT&T will provide assistance or equivalent facilitation when requested in advance by the government. For training delivered via instructor-led and non-instructor online web-based courses, AT&T will provide equivalent Internet reporting capabilities to trainees with disabilities. For

2.2 Optional EIS Services [L.29(2)(b); M.1.1; M.4; M.5; C.1.8.1]

[illegible]

2.2.1.1 Optical Wavelength Service [L.29.2.1; M.2.1; C.2.1.3]

Agencies Benefit from Our Extensive OWS Network Deployment

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

systems that support multiple SONET and Ethernet standards-compliant signals. This level of system capacity will enable agencies to benefit from our competitively priced support of high-performance applications. We can respond quickly to bandwidth demands, giving agencies unprecedented flexibility to handle large unexpected traffic surges.

2.2.1.1.1 How AT&T Will Provide Proposed Services and Features **[L.29.2.1; M.2.1]**

2.2.1.1.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

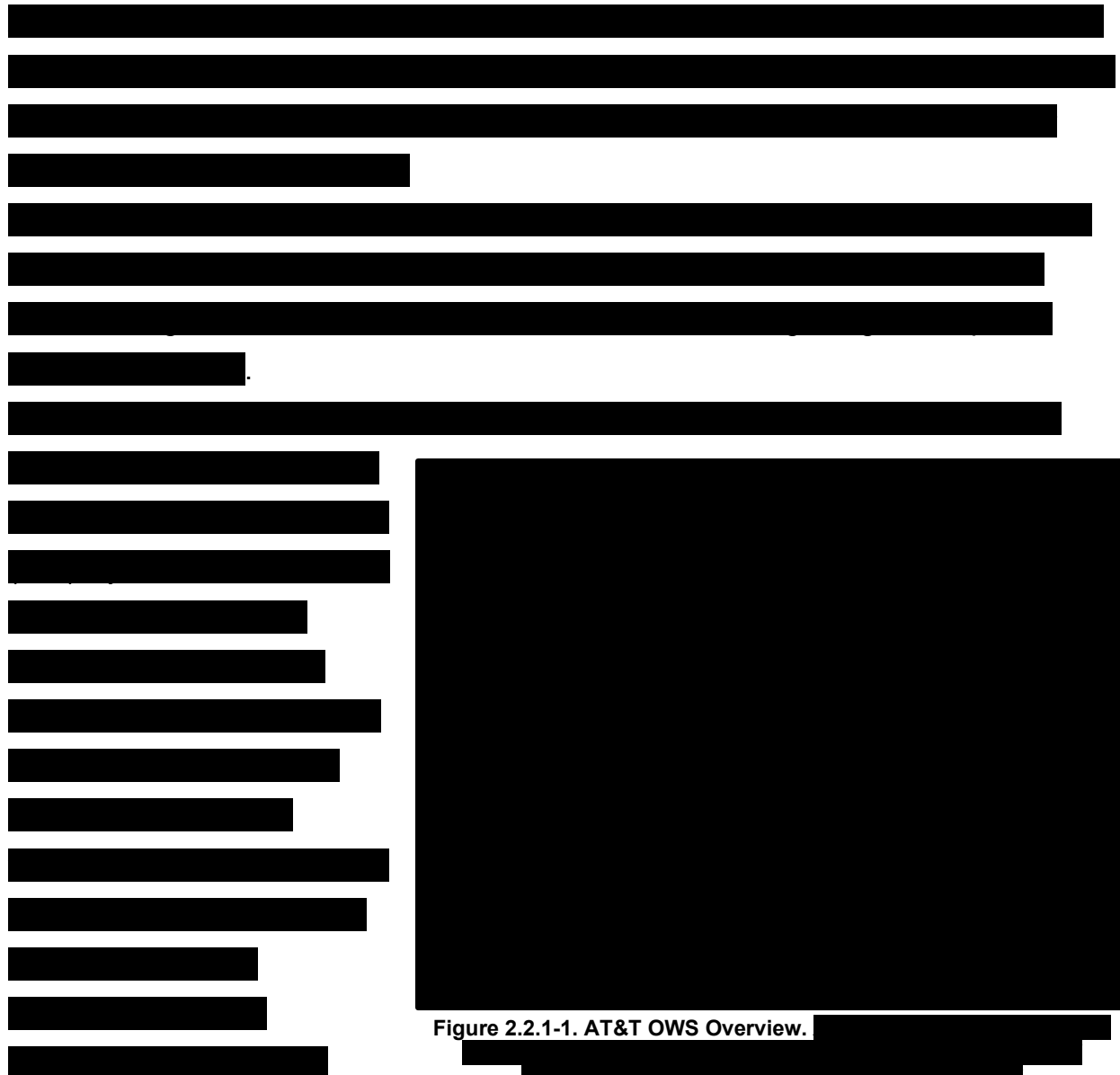


Figure 2.2.1-1. AT&T OWS Overview.

meet EIS service requirements as shown in **Figure 2.2.1-1** and **Table 2.2.1-1**.

Table 2.2.1-1. OWS Overview Description. Agencies can use the AT&T OWS to achieve important EIS objectives, and benefit from a technology that is highly reliable, survivable, highly secured, and interoperable with other services, easy to provision, and fully maintained to meet present and future requirements.

Architectural Components	Description
Functional Components	
Support of various SONET and ethernet standards-compliant 1, 2.5, 10, 40, and 100 Gbps signals	
Optical transparent network	
Supports multiple topologies	
Technical Components	
Domestic wavelengths	
Metro wavelength services	
Transmission rates	
Clock transparency	
Operational Components	
High reliability	
High survivability	
Maximum security and information assurance	
Interoperability	
Provisioning	
End-to-end Maintenance	

Architectural Components	Description
Network Components	
Inter-city extensibility and reach	[REDACTED]
Metropolitan fiber	[REDACTED]
Intelligent optical switches	[REDACTED]

2.2.1.1.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our approach and architecture for delivering OWS delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.2.1-2**.

Table 2.2.1-2. OWS QoS. OWS is fully compliant, and provides the robust scalability, high reliability, and strong resilience sought by GSA and agencies. Service quality is confirmed by centralized monitoring of all optical network elements and supporting physical infrastructures.

Architectural Components	Description
Compliance	
Demonstrated compliance	[REDACTED] Section 2.2.1.1.2.
Scalability	
AT&T network coverage	[REDACTED]
WDM	[REDACTED]
Reliability	
Policies and programs	[REDACTED]
Network diversity	[REDACTED]
Resilience	
Protection topologies	[REDACTED]
High survivability	[REDACTED]

2.2.1.1.1.3 [REDACTED]

See **Section 1.3** for AT&T service coverage for OWS.

2.2.1.1.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.1.1.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

OWS has no service-specific requirements indicated in the RFP.

2.2.1.1.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for OWS are protected from information breaches, unauthorized access and supply [REDACTED]

2.2.1.1.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3)]

Our proposed [REDACTED]

Table 2.2.1-3 [REDACTED]

Table 2.2.1-3. Approach to External Traffic Routing Requirements. *Agencies will receive services that operate* [REDACTED]

Requirement	Compliance Description
Methodology for Identifying AT&T Participating Agency Traffic for Each Affected Service [M.2.1.4.c.i]	[REDACTED] Section 1.4.3.1.
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 [M.2.1.4.c.ii]	[REDACTED] Section 1.4.3.2.
Technical Approach to Notify DHS If Any Non-Participating Agency Traffic Will Be Redirected Through DHS EINSTEIN Enclaves [M.2.1.4.c.iii]	[REDACTED] Section 1.4.3.3.
Control Mechanisms to Ensure the Identification and Redirection of Participating Agency Traffic Cannot Be Inadvertently or Maliciously By-Passed [M.2.1.4.c.iv]	[REDACTED] Section 1.4.3.4.
Sensing and Control Mechanisms to Ensure the Redirection of Traffic is Failsafe [M.2.1.4.c.v]	[REDACTED] Section 1.4.3.5.
Location of AT&T Certified Facilities [M.2.1.4.c.vi]	[REDACTED] Section 1.4.3.6.
Availability of TS/SCI Cleared Personnel for "Smart-Hands" Service of DHS Supplied Equipment [M.2.1.4.c.vii]	[REDACTED] 1.4.3.7.
Instrumentation to Measure Transport SLA KPIs [M.2.1.4.c.viii]	[REDACTED] Section 1.4.3.8.

2.2.1.1.2 Technical Response for OWS [L.29.2.1; M.2.1]

2.2.1.1.2.1 Service Description and Functional Definition [L.29.2.1; C.2.1.3.1; C.2.1.3.1.1]

Agencies will receive a solution that provides the full service scope and functional capabilities, as described in **Table 2.2.1-4**, and described previously in **Section 2.2.1.1.1.1**.

2.2.1.1.2.2 Standards [L.29.2.1; C.2.1.3.1.2]

AT&T will comply with all standards listed in RFP Section C.2.1.3.1.2 and with other standards referenced by the listed standards, as applicable.

AT&T OWS Fiber Protection	
■	[REDACTED]
	[REDACTED]
■	[REDACTED]
	[REDACTED]

Table 2.2.1-4. OWS Service Scope and Functional Capabilities.

[REDACTED]	
[REDACTED]	
Solution Element	Description
CONUS wavelengths	[REDACTED]
Metro wavelength services	[REDACTED]
Transmission rates	[REDACTED]
Clock transparency	[REDACTED]
Proprietary technology	[REDACTED]

2.2.1.1.2.3 Connectivity [L.29.2.1; C.2.1.3.1.3]

AT&T will comply with all connectivity instances listed in RFP Section C.2.1.3.1.3, as applicable.

2.2.1.1.2.4 Technical Capabilities [L.29.2.1; C.2.1.3.1.4]

Agencies will receive OWS that meets all mandatory technical capabilities, and optional technical capabilities as applicable. All proposed technical capabilities are described in **Table 2.2.1-5**, and described previously in **Section 2.2.1.1.1.1**.

Table 2.2.1-5. OWS Technical Capabilities. Agencies will receive an AT&T

#	Technical Capability		Description
1.	Non-domestic wavelengths connection (optional)		
2.	Domestic wavelengths connection		
3.	Metro wavelength services connection		
1.	Transmission rates		
2.	Clock transparency		
3.	Protocol transparency – metro		
4.	Protocol transparency – domestic and non-domestic (optional)		
5.	Byte transparency		
6.	Concatenation		
7.	Channelization (optional)		
8.	Wavelength delivery		
9.	Access methods		

#	Technical Capability		Description
10.	Government-furnished property/SRE		<ul style="list-style-type: none"> Government-furnished property/SRE Government-furnished property/SRE Government-furnished property/SRE Government-furnished property/SRE
11.	Efficient transport		<ul style="list-style-type: none"> Efficient transport

2.2.1.1.2.5 Features [L.29.2.1; C.2.1.3.2]

Agencies will receive an established OWS that meets all mandatory features, and optional features as applicable. All proposed features are described in **Table 2.2.1-6**, and described previously in **Section 2.2.1.1.1.1**.

Table 2.2.1-6. OWS Features. *Agencies will receive*

#	Feature		Description
1.	CNM – level 1 (optional)		CNM – level 1 (optional)
2.	CNM – level 2 (optional)		CNM – level 2 (optional)
3.	Equipment protection 1:1 – GFP/SRE		Equipment protection 1:1 – GFP/SRE
4.	Equipment protection 1+1 – GFP/SRE		Equipment protection 1+1 – GFP/SRE
5.	Equipment protection – network side		Equipment protection – network side
6.	Geographical diversity wavelengths		Geographical diversity wavelengths
7.	Protected non-domestic and OCONUS wavelength (optional)		Protected non-domestic and OCONUS wavelength (optional)
8.	Protected CONUS wavelength (optional)		Protected CONUS wavelength (optional)
9.	Protected metro wavelength		Protected metro wavelength

#	Feature		Description

2.2.1.1.2.6 Interfaces [L.29.2.1; C.2.1.3.3]

The AT&T OWS is compatible with interfaces in RFP Section C.2.1.1.3, as applicable.

2.2.1.1.2.7 Performance Metrics [L.29.2.1; C.2.1.3.4]

The AT&T [REDACTED]

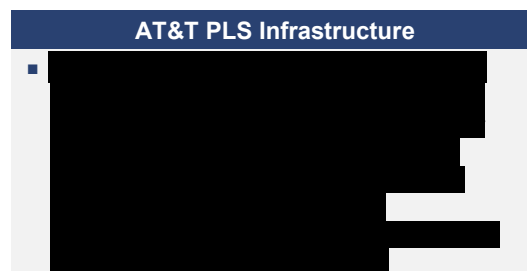
[REDACTED]

[REDACTED]

[REDACTED]

2.2.1.2 Private Line Service [L.29.2.1; M.2.1; C.2.1.4]

Agencies can maintain continuity with existing PLS services when transitioning to EIS. PLS provides a global, dedicated, high-speed, reliable solution, featuring a wide variety of bandwidth options. With the AT&T



PLS solution, agencies can choose from [REDACTED], providing any Layer 1 solution they may require. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.2.1.2.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.1.2.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

The AT&T proposed architecture and services, as shown in **Figure 2.2.1-2** and **Table 2.2.1-7**, meet [REDACTED]

[REDACTED]

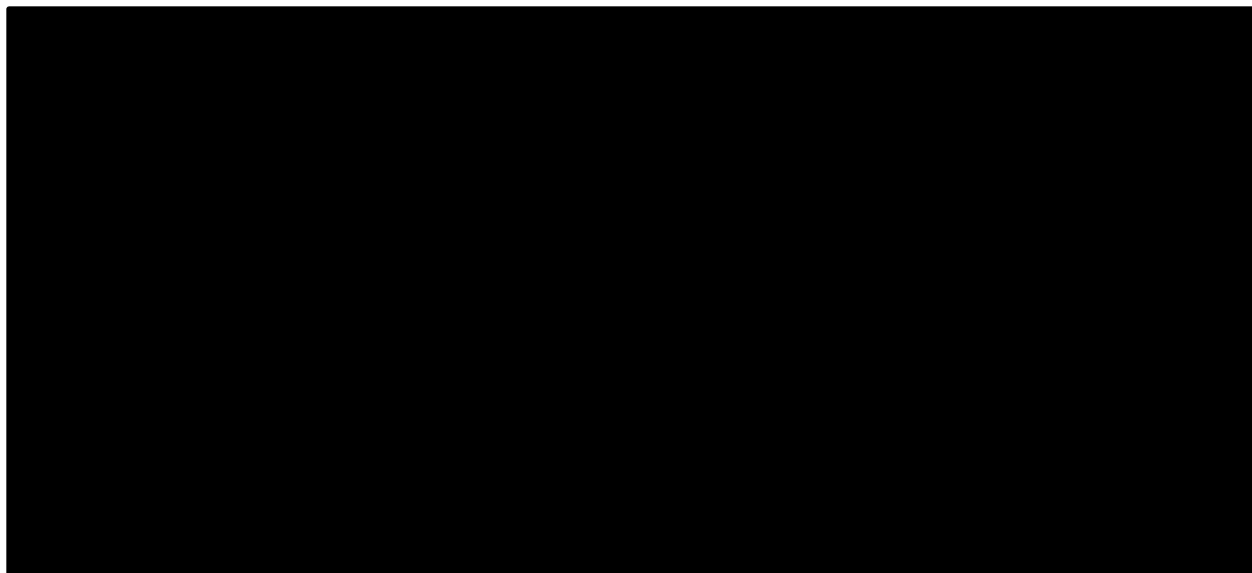


Figure 2.2.1-2. PLS Overview.

Table 2.2.1-7. PLS Overview Description. PLS services are provided over a Layer 1 legacy TDM/optical and next generation optical network of

Architectural Components	Description
Overall PL Network Architecture	
AT&T EIS access and transport network	■ [Redacted]
	■ [Redacted]
	■ [Redacted]
	■ [Redacted]
	■ [Redacted]
	■ [Redacted]
Functional Components	
Intelligent optical network	■ [Redacted]
	■ [Redacted]
SONET/OTN metro networks	■ [Redacted]
	■ [Redacted]

Architectural Components	Description
Multi-service provisioning platform NEs	
TDM access networks	
Digital cross-connect systems (DCS)	
International PDH/SDH networks	

2.2.1.2.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our approach and architecture for delivering PLS will deliver compliant, scalable, reliable, and resilient service as shown in **Table 2.2.1-8**.

Table 2.2.1-8. PLS QoS. The AT&T PLS is fully compliant with all mandatory service and functional requirements, standards, connectivity, technical capabilities, features, interfaces, and performance metrics.

Architectural Components	Description
Compliance	
Demonstrated capability	<ul style="list-style-type: none"> Section 2.2.1.2.2
Scalability	
OTN technology	
Extensive physical footprint	
Reliability	
Intelligent optical network, SONET and optical NEs	<ul style="list-style-type: none"> Backbone and metro NEs deployed in fully redundant mesh physical and logical architectures using NEBS-compliant carrier-grade NEs certified by AT&T Labs
Resilience	
Distributed restoration	

2.2.1.2.1.3 Service Coverage (CBSA-Dependent) [L.29.2.1(C); M.2.1(3); C.1.3]

See **Section 1.3** for AT&T service coverage for PLS.

2.2.1.2.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.1.2.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

While PLS has no service-specific requirements indicated in the RFP.

2.2.1.2.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for PLS are protected from information breaches, unauthorized access and supply chain risks

2.2.1.2.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3)]

Our proposed architecture meets all external traffic routing requirements applicable to PLS. **Table 2.2.1-9** provides detailed references to our approach.

Table 2.2.1-9. Approach to External Traffic Routing Requirements.

Requirement	Compliance Description
Methodology for Identifying AT&T Participating Agency Traffic for Each Affected Service [M.2.1.4.c.i]	Section 1.4.3.1.
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 [M.2.1.4.c.ii]	Section 1.4.3.2.
Technical Approach to Notify DHS If Any Non-Participating Agency Traffic Will Be Redirected Through DHS EINSTEIN Enclaves [M.2.1.4.c.iii]	Section 1.4.3.3.
Control Mechanisms to Ensure the Identification and Redirection of Participating Agency Traffic Cannot Be Inadvertently or Maliciously By-Passed [M.2.1.4.c.iv]	The two control mechanisms for safeguarding agency traffic against inadvertent or malicious bypass are Demarcation and System Access. For more detail on the AT&T control mechanisms, see Section 1.4.3.4.
Sensing and Control Mechanisms to Ensure the Redirection of Traffic is Failsafe [M.2.1.4.c.v]	Section 1.4.3.5.
Location of AT&T Certified Facilities [M.2.1.4.c.vi]	Section 1.4.3.6.
Availability of TS/SCI Cleared Personnel for "Smart-Hands" Service of DHS Supplied Equipment [M.2.1.4.c.vii]	Section 1.4.3.7.
Instrumentation to Measure Transport SLA KPIs [M.2.1.4.c.viii]	Section 1.4.3.8.

2.2.1.2.2 Technical Response for PLS [L.29.2.1; M.2.1]

2.2.1.2.2.1 Service Description and Functional Definition [L.29.2.1; C.2.1.4.1; C.2.1.4.1.1]

Agencies will receive a solution that provides full service scope and functional capabilities, as described in **Table 2.2.1-10**, and described previously in **Section 2.2.1.2.1.1**.

Table 2.2.1-10. PLS Service Scope and Functional Capabilities.

Service Scope/ Delivery Approach	Description
Global network reach	
Easy provisioning	
Reliable network	
Survivability	
Extensibility	
Proprietary technology	

2.2.1.2.2.2 Standards [L.29.2.1; C.2.1.4.1.2]

AT&T will comply with all standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.2.1.2.2.3 Connectivity [L.29.2.1; C.2.1.4.1.3]

AT&T will comply with all connectivity instances listed in the RFP as applicable.

2.2.1.2.2.4 Technical Capabilities [L.29.2.1; C.2.1.4.1.4]

Agencies will receive a PLS that meets all mandatory technical capabilities. All proposed technical capabilities are described in **Table 2.2.1-11**,

Section 2.2.1.2.1.1.

Table 2.2.1-11. PLS Technical Capabilities. Agencies will receive services

#	Technical Capability	Description
1.	Routing requirements	
2.	Transparency	

#	Technical Capability		Description
3.	Data transparency		
Supported Categories of Data Rates			
1.	DS0		
2.	T1 and T3		
4.&5.	E1 and E3		
8.	SONET OC-3		
9.	OC-12		
10.	OC-48		
11.	OC-192		
14.	Analog Line (4K)		
16.	Fractional T3		

2.2.1.2.2.5 Features [L.29.2.1; C.2.1.4.2]

Agencies will receive a verified and validated PLS

Table 2.2.1-12,

Section 2.2.1.2.1.1.

Table 2.2.1-12. PLS Features. Agencies will receive services that meet the required set of features provided by layer 1 digital bridging devices, SONET and TDM network elements, and custom engineering and provisioning practices.

#	Feature		Description
RFP Required Features			
1.	Multipoint connection		
2.	Special routing		

2.2.1.2.2.6 Interfaces [L.29.2.1; C.2.1.4.3]

The AT&T PLS is compatible with interfaces in RFP Section C.2.1.4.3, as applicable.

2.2.1.2.2.7 Performance Metrics [L.29.2.1; C.2.1.4.4]

2.2.1.3 Synchronous Optical Network Service [L.29.2.1; M.2.1; C.2.1.5]

The AT&T Synchronous Optical Network Service (SONETS) is a self-healing optical fiber network service that will provide highly reliable, highly secured, and dedicated connectivity for agency voice, data, telemetry, video, or multimedia and encrypted communications.

2.2.1.3.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.1.3.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

AT&T SONETS offers Layer 1 optical transport in access and core networks. The optical layer provides the foundation of transport services for metro and LH applications. **Figure 2.2.1-3** identifies key elements of the AT&T SONETS, including reporting capabilities, access options, and routing control tools. Our proposed architecture and services meet EIS service requirements shown in **Table 2.2.1-13**.

The AT&T PLS meets all KPIs listed in RFP Section C.2.1.4.4. EIS Compliant AT&T SONETS Capabilities	
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]

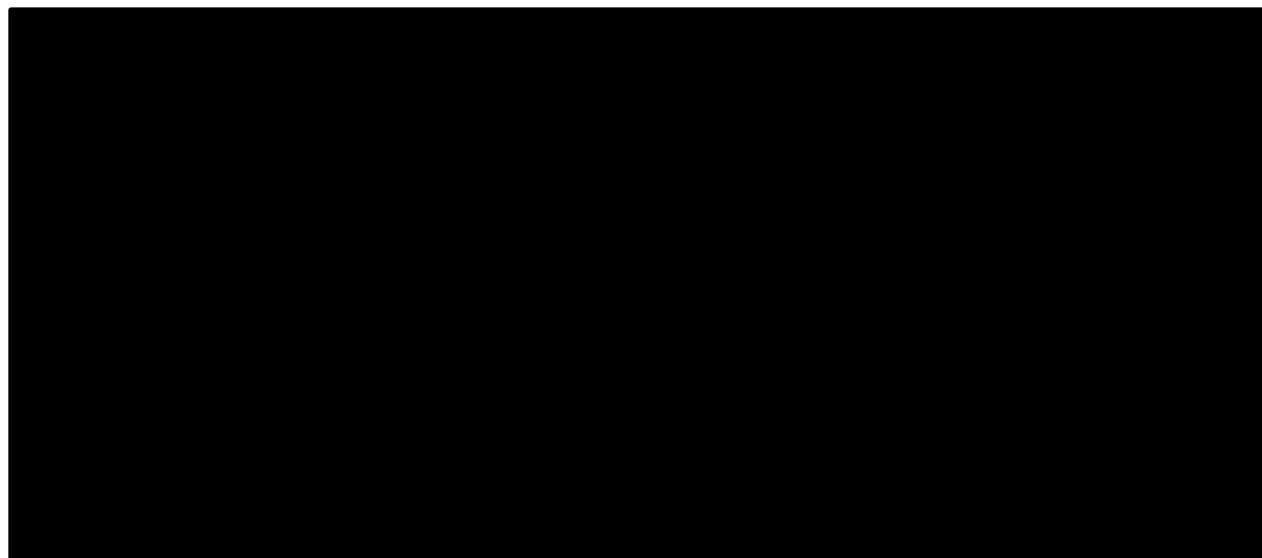


Figure 2.2.1-3. SONET Overview.

Table 2.2.1-13. SONET Overview Description. AT&T SONET service has received

Architectural Components	Description
Functional Components	
SONET SDP to SDP service	
SONET PoP-to-PoP service	
SONET metro and long-haul ring services	
Linear APS	
UPSR	
BLSR	
Intelligent optical switches	
DCS	
SMPP	
Technical Components	
Geographic coverage	
Protection	
Performance monitoring	
Operational Components	
Performance	
Reliability	
Survivability	
Interoperability	
Provisioning	
End-to-end maintenance	

Architectural Components	Description
Network Components	
AT&T core network	
Inter-city extensibility and reach	
Metropolitan fiber	

2.2.1.3.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our approach and architecture for delivering SONET is compliant, reliable, scalable, and resilient, as shown in **Table 2.2.1-14**.

Table 2.2.1-14. SONETS QoS. AT&T SONETS is fully compliant, and provides the high reliability, robust scalability, and strong resilience sought by agencies. Service quality is corroborated through AT&T recognition

Architectural Components	Description
Compliance	
Private Line Interoffice Connection (PL-IOC)	Section 2.2.1.3.2
Private Line Service (PLS)	Section 2.2.1.3.2
Dedicated Ring Service (DRS)	Section 2.2.1.3.2
Scalability	
Expansion platform	
Expandability	
Network diversity	
Reliability	
AT&T network survivability protocol	
Power redundancy	
Management and monitoring	
Resilience	
AT&T backbone network	

Architectural Components	Description
Protection against hard failures within AT&T network	[REDACTED]
Network disaster recovery	[REDACTED]
Maximum security and information	[REDACTED]

2.2.1.3.1.3 [REDACTED]

See **Section 1.3** for AT&T service coverage for SONETS.

2.2.1.3.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.1.3.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

SONETS has no service-specific requirements indicated in the RFP.

2.2.1.3.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for SONETS are protected from information breaches, unauthorized access and supply chain risks [REDACTED]

2.2.1.3.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3)]

Our proposed architecture meets all external traffic routing requirements applicable to SONETS. **Table 2.2.1-15** provides detailed references to our approach.

Table 2.2.1-15. Approach to External Traffic Routing Requirements. Agencies will receive services that operate on a network that meets all external traffic routing requirements as described in the AT&T network architecture.

Requirement	Compliance Description
Methodology for Identifying AT&T Participating Agency Traffic for Each Affected Service [M.2.1.4.c.i]	[REDACTED] Section 1.4.3.1.
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 [M.2.1.4.c.ii]	[REDACTED] Section 1.4.3.2.

Requirement	Compliance Description
Technical Approach to Notify DHS If Any Non-Participating Agency Traffic Will Be Redirected Through DHS EINSTEIN Enclaves [M.2.1.4.c.iii]	Section 1.4.3.3.
Control Mechanisms to Ensure the Identification and Redirection of Participating Agency Traffic Cannot Be Inadvertently or Maliciously By-Passed [M.2.1.4.c.iv]	Section 1.4.3.4.
Sensing and Control Mechanisms to Ensure the Redirection of Traffic is Failsafe [M.2.1.4.c.v]	Section 1.4.3.5.
Location of AT&T Certified Facilities [M.2.1.4.c.vi]	Section 1.4.3.6.
Availability of TS/SCI Cleared Personnel for “Smart-Hands” Service of DHS Supplied Equipment [M.2.1.4.c.vii]	Section 1.4.3.7.
Instrumentation to Measure Transport SLA KPIs M.2.1.4.c.viii]	Section 1.4.3.8.

2.2.1.3.2 Technical Response for SONETS [L.29.2.1; M.2.1]

2.2.1.3.2.1 Service Description and Functional Definition [L.29.2.1; C.2.1.5.1; C.2.1.5.1.1]

Agencies will receive a solution that provides the full service scope and functional capabilities, as described in **Table 2.2.1-16** and described previously in

Section 2.2.1.3.1.1.

Table 2.2.1-16. SONETS Scope and Functional Capabilities. Agencies can use

Solution Element	Description
AT&T Private Line Inter-office Channel (PL-IOC)	
AT&T SONET Private Line Service (PLS)	

Solution Element	Description
Dedicated Ring Service (DRS)	[REDACTED]
Proprietary technology	[REDACTED]

2.2.1.3.2.2 Standards [L.29.2.1; C.2.1.5.1.2]

AT&T will comply with all standards listed in RFP Section C.2.1.5.1.2 and with other standards referenced by the listed standards, as applicable.

2.2.1.3.2.3 Connectivity [L.29.2.1; C.2.1.5.1.3]

AT&T will comply with all connectivity instances listed in the RFP as applicable.

2.2.1.3.2.4 Technical Capabilities [L.29.2.1; C.2.1.5.1.4]

Agencies will receive SONETS that meets all mandatory technical capabilities. All proposed technical capabilities are described in **Table 2.2.1-17** and described previously in **Section 2.2.1.3.1.1**.

Table 2.2.1-17. SONETS Technical Capabilities. Agencies will receive with AT&T SONETS a competitively priced way to transport large amounts of data between large and small offices to the agencies' headquarters through a SONET OCN circuit with add/drop multiplexing.

#	Technical Capability		Description
1.	Coverage	[REDACTED]	[REDACTED]
2.	Gateway (optional)	[REDACTED]	[REDACTED]
3.	Network topology	[REDACTED]	[REDACTED]
4.	Protection customer and Protection network	[REDACTED]	[REDACTED]
5.	Transmux capabilities	[REDACTED]	[REDACTED]
6.	Concatenation (optional)	[REDACTED]	[REDACTED]
7.	Performance monitoring	[REDACTED]	[REDACTED]
8.	Synchronization and timing methods	[REDACTED]	[REDACTED]
10.	Next generation SONET	[REDACTED]	[REDACTED]
11.	Other Support	[REDACTED]	[REDACTED]

2.2.1.3.2.5 Features [L.29.2.1; C.2.1.5.2]

Agencies will receive established SONETS that meets all mandatory features. All proposed features are described in **Table 2.2.1-18** and described previously in **Section 2.2.1.3.1.1**.

Table 2.2.1-18. SONET Features. Agencies will be able to use AT&T SONETS, which meets all required features, to consolidate Ethernet, data, video, and voice traffic among agencies' locations and the AT&T central offices on a single, fail-safe platform.

Feature		Description
RFP Required Features		
Channelization		
Synchronized services (optional)		
Performance		
Equipment protection		
Framing for electrical interfaces		
Geographic diverse protection		
Local and remote Node multiplexing		

2.2.1.3.2.6 Interfaces [L.29.2.1; C.2.1.5.3]

The AT&T SONETS is compatible with interfaces in RFP Section C.2.1.5.3, as applicable.

2.2.1.3.2.7 Performance Metrics [L.29.2.1; C.2.1.5.4]

The AT&T SONETS meets all KPIs listed in RFP Section C.2.1.5.4.

2.2.1.4 Dark Fiber Service [L.29.2.1; M.2.1; C.2.1.6]

Agencies will receive the AT&T flexible and scalable DFS, which offers broad geographical coverage, modern infrastructure, and flexible configuration capabilities that will enable the customer agencies to meet mission needs.

2.2.1.4.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.1.4.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

Dark fiber is an optical fiber infrastructure (cabling and repeaters) that enables agencies to design their own optical networks, connect their own electronics to provide transport on fiber strands, and modify their networks as needed to meet mission requirements.

The AT&T DFS will provide physical strands of fiber plant between agency service delivery points (SDP) and may also be terminated to an AT&T colocation.

DFS offers simple point-to-point connections between two locations as well as configurations that interconnect multiple locations and can include intermediate amplification or repeater locations to extend reach.

Our proposed architecture and services meet EIS service requirements as shown in **Figure 2.2.1-4** and **Table 2.2.1-19**.

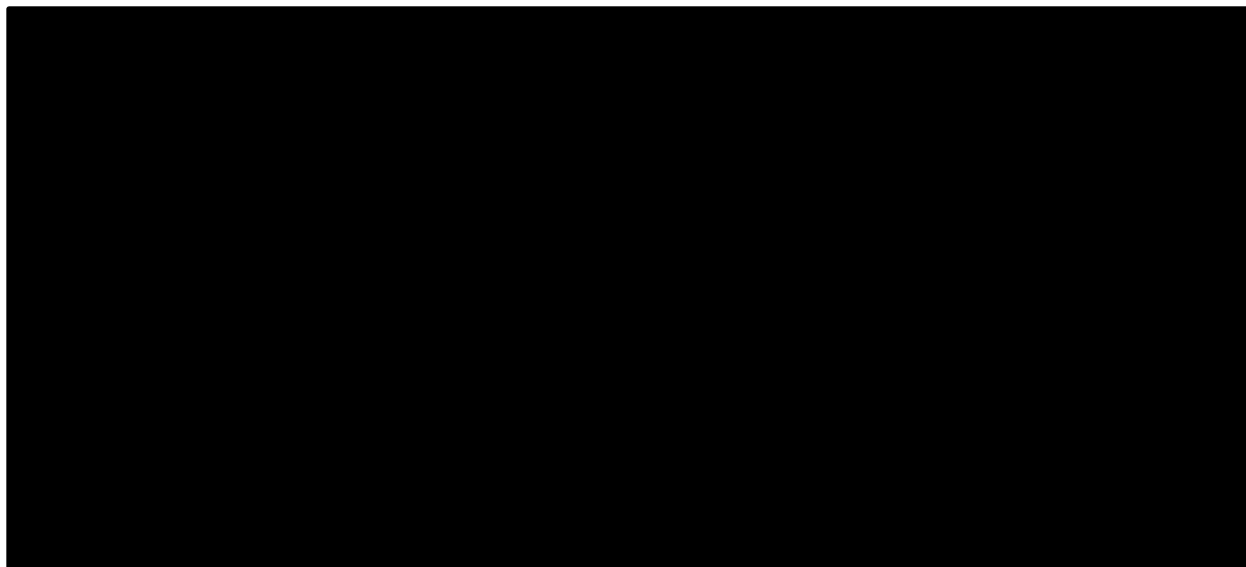


Figure 2.2.1-4. DFS Overview.

Table 2.2.1-19. DFS Overview Description. *DFS components give agencies extensive fiber footprint, a large subcontractor ecosystem to augment our coverage, and construction capabilities to splice together or extend an existing network.*

Architectural Components	Description
Functional Components	
Geographical coverage	<ul style="list-style-type: none"> [Redacted] [Redacted] [Redacted]
Configuration options	<ul style="list-style-type: none"> [Redacted] [Redacted] [Redacted] [Redacted] [Redacted]

Architectural Components	Description
Fiber service delivery point	[REDACTED]
Optical fiber	[REDACTED]
Ducting	[REDACTED]
Future growth	[REDACTED]
Technical Components	
Geographical coverage	[REDACTED]
Configuration alternatives	[REDACTED]
Channel count	[REDACTED]
Required optical characteristics	[REDACTED]
Operational Components	
EIS services verification criteria	[REDACTED]
Service components	[REDACTED]
Network Components	
Gateways	[REDACTED]
Amplification	[REDACTED]
Fiber deployed	[REDACTED]

AT&T offers a wide range of coverage and service [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.2.1.4.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our approach and architecture for delivering DFS delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.2.1-20**.

Table 2.2.1-20. DFS QoS. DFS is fully compliant, and provides the robust scalability, high reliability, and strong resilience sought by GSA and its client agencies.

Architectural Components	Description
Compliance	
Demonstrated capability	<ul style="list-style-type: none"> Section 2.2.1.4.2
Scalability	
Future growth	<ul style="list-style-type: none">
Reliability	
Maintenance	<ul style="list-style-type: none">
Established management process	<ul style="list-style-type: none">
Resilience	
Diversified infrastructure	<ul style="list-style-type: none">

2.2.1.4.1.3

See **Section 1.3** for the AT&T service coverage for DFS.

2.2.1.4.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.1.4.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

While DFS has no service-specific requirements indicated in the RFP.

2.2.1.4.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

. **Section 1.4** describes AT&T's security approach for this architecture.

2.2.1.4.2 Technical Response for DFS [L.29.2.1; M.2.1]

2.2.1.4.2.1 Service Description and Functional Definition [L.29.2.1; C.2.1.6.1; C.2.1.6.1.1]

Agencies will receive a solution that provides full service, scope, and functional capabilities, described in **Table 2.2.1-22** and described previously in

Section 2.2.1.4.1.1.

Table 2.2.1-22. AT&T DFS Service Scope and Functional Capabilities. Agencies will receive service capabilities proven on *Networx* to meet DFS service description and functional requirements. All of these capabilities are provided by AT&T nationwide rights of way, use of the latest fiber optic cable technologies, and professional services management experience.

Solution Element	Description
Fiber route right to use	<ul style="list-style-type: none"> Allows the agency the unconditional right to use fiber route, which provides capacity such as a fiber pair in the fiber-optic cable or the entire fiber-optic cable
Optronics flexibility	<ul style="list-style-type: none"> Allows agencies that acquire dark fiber to either provide their own optical equipment or acquire as SRE.
Managed network service flexibility	<ul style="list-style-type: none"> Can be selected by agencies who prefer not to design, implement, and manage their own Dark Fiber networks (additional fees may apply)
Proprietary technology	<ul style="list-style-type: none"> No proprietary AT&T technology used

2.2.1.4.2.2 Standards [L.29.2.1; C.2.1.6.1.2]

AT&T will comply with all standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.2.1.4.2.3 Connectivity [L.29.2.1; C.2.1.6.1.3]

AT&T will comply with all connectivity instances listed in the RFP as applicable.

2.2.1.4.2.4 Technical Capabilities [L.29.2.1; C.2.1.6.1.4]

[REDACTED]

[REDACTED]

[REDACTED] **Section 2.2.1.4.1.1.**

Table 2.2.1-23. DFS Technical Capabilities. Agencies will receive an EIS-compliant service to meet required technical capabilities, provided by the AT&T footprint, and network design and construction specialists.

#	Technical Capability	Description
1.	Geographical coverage	[REDACTED]
2.	Configuration alternatives	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Hybrid Configurations – Combine network topology configurations into hybrid custom-tailored solutions		

#	Technical Capability		Description
1)	Fiber service delivery point		<ul style="list-style-type: none"> [REDACTED] [REDACTED]
2)	Ducting		<ul style="list-style-type: none"> [REDACTED]
3)	Future growth (optional)		<ul style="list-style-type: none"> [REDACTED]
4)	Channel count		<ul style="list-style-type: none"> [REDACTED]
5)	Gateways		<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
6)	Service components		<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED]

2.2.1.4.2.5 Features [L.29.2.1; C.2.1.6.2]

Agencies will receive established DFS that meets all mandatory and optional features as described in **Table 2.2.1-24** and described previously in **Section 2.2.1.4.1.1**.

Table 2.2.1-24. DFS Features. Agencies will acquire access to an EIS-compliant service that meets its feature requirements and is customizable. Features are supported by our colocation product set, worldwide footprint of facilities, diversity design and implementation capabilities, and construction expertise.

#	Feature		Description
RFP Required Features			
1.	Colocation service		<ul style="list-style-type: none"> [REDACTED]
2.	Duct (optional)		<ul style="list-style-type: none"> [REDACTED]
3.	Dark fiber local loop (optional)		<ul style="list-style-type: none"> [REDACTED]
4.	Diverse route single drop (optional)		<ul style="list-style-type: none"> [REDACTED]

#	Feature		Description
5.	Diverse route dual drop (Optional)		
6.	Inter-city connectivity (optional)		
7.	Multiple duct (optional)		
8.	Splicing		
9.	Off-net laterals		

2.2.1.4.2.6 Interfaces [L.29.2.1; C.2.1.6.3]

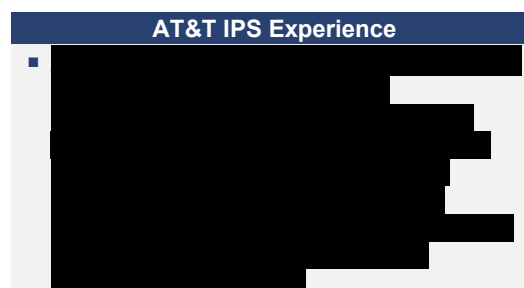
The AT&T DFS is compatible with interfaces in RFP Section C.2.1.6.3, as applicable.

2.2.1.4.2.7 Performance Metrics [L.29.2.1; C.2.1.6.4]

The AT&T DFS meets all KPIs listed in RFP Section C.2.1.6.4.

2.2.1.5 Internet Protocol Service [L.29.2.1; M.2.1; C.2.1.7]

Agencies will access an Internet Protocol Service (IPS) with comprehensive layered security and proactive, 24x7 network monitoring and maintenance.



2.2.1.5.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.1.5.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

The AT&T IPS provides agencies with a wide range of connectivity requirements that support IPv4 and IPv6 to enable government users' access to the Internet, government-wide intranets, and extranets. IPS uses the TCP/IP protocol suite to interconnect GFP/SRE with other government networks and the public ISP networks by providing transport of IP packets. The AT&T proposed architecture and services meet EIS service requirements as shown in **Figure 2.2.1-5** and **Table 2.2.1-25**.

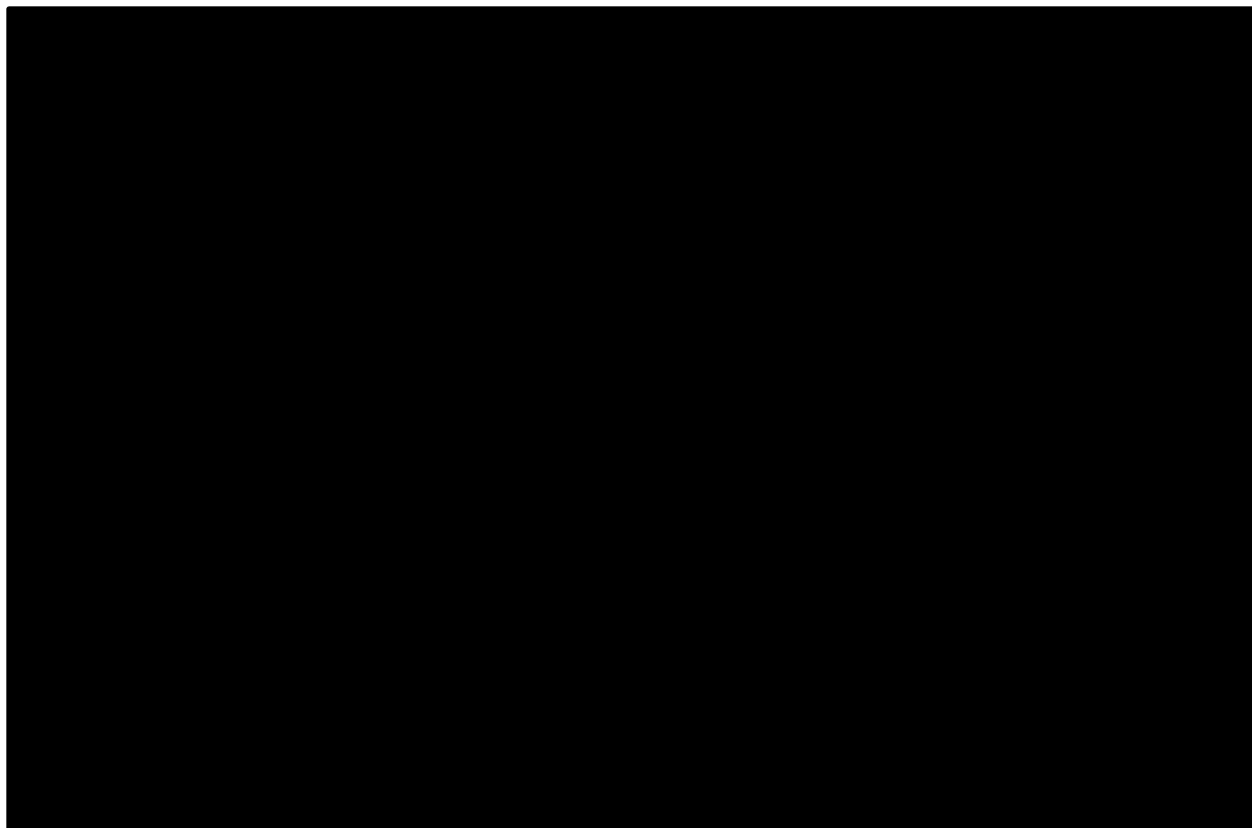


Figure 2.2.1-5. AT&T IPS Network Architecture.

Table 2.2.1-25. IPS Overview Description. *AT&T backbone and edge routers, combined with our global footprint, comprehensive peering, and wide range of access types, along with diversity options for critical sites, provide a scalable and robust IPS to agencies.*

Architectural Components	Description
Functional Components	
AT&T IP/MPLS backbone and edge routers	
Global footprint	
Connectivity	
Access types	
Redundancy options	
Technical Components	

Architectural Components	Description
Domain Name System (DNS) option	<ul style="list-style-type: none"> ■ [Redacted] ■ [Redacted] ■ [Redacted] ■ [Redacted]
Operational Components	
Network operations	<ul style="list-style-type: none"> ■ [Redacted]
Routing architecture	<ul style="list-style-type: none"> ■ [Redacted]
High reliability	<ul style="list-style-type: none"> ■ [Redacted]
High survivability	<ul style="list-style-type: none"> ■ [Redacted]
Full interoperability	<ul style="list-style-type: none"> ■ [Redacted]
Efficient provisioning	<ul style="list-style-type: none"> ■ [Redacted]
End-to-end maintenance	<ul style="list-style-type: none"> ■ [Redacted]
Network Components	
Intelligent optical switches	<ul style="list-style-type: none"> ■ [Redacted]
Inter-city fiber extensibility and reach	<ul style="list-style-type: none"> ■ [Redacted]
Metropolitan fiber	<ul style="list-style-type: none"> ■ [Redacted]
Separation of services	<ul style="list-style-type: none"> ■ [Redacted]

2.2.1.5.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our approach and architecture for delivering IPS delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.2.1-26**.

Table 2.2.1-26. IPS QoS. *IPS is fully compliant, and provides the robust scalability, high reliability, and strong resilience sought by GSA and agencies. All AT&T hardware and software elements in the network are rigorously tested in AT&T Labs before they are deployed.*

Architectural Components	Description
Compliance	
Demonstrated capability	■ [REDACTED]
Scalability	
Expansion platform	■ [REDACTED]
Non-traditional space	■ [REDACTED]
Network capacity	■ [REDACTED]
Reliability	
Backbone node redundancy	■ [REDACTED]
Access redundancy	■ [REDACTED]
Automatic load balancing	■ [REDACTED]
CPE redundant configuration	■ [REDACTED]
Resilience	
Optical mesh self-healing network	■ [REDACTED]

See **Section 1.3** for AT&T service coverage for IPS.

2.2.1.5.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.1.5.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

IPS security related capabilities are indicated in RFP Section C.2.1.7.1.4, and are addressed in proposal **Section 2.2.1.5.2.4**. **Table 2.2.1-27** delineates additional service-specific security capabilities delivered to agencies.

Table 2.2.1-27. IPS Service-Specific Security Capabilities. Agencies will receive highly secured services based on our overall architecture and service-specific capabilities.

Capability	Description
Security experience	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Dedicated security operation center	<ul style="list-style-type: none"> [REDACTED]
Building security	<ul style="list-style-type: none"> [REDACTED]
Network security	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

2.2.1.5.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for IPS are protected from information breaches, unauthorized access and supply chain risks [REDACTED]

[REDACTED]

[REDACTED].

2.2.1.5.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3)]

Our proposed architecture meets all external traffic routing requirements applicable to IP service. **Table 2.2.1-28** provides detailed references to our approach.

Table 2.2.1-28. Approach to External Traffic Routing Requirements. Agencies will receive services that operate on a network that meets all external traffic routing requirements as described in the AT&T network architecture.

Requirement	Compliance Description
Methodology for Identifying AT&T Participating Agency Traffic for Each Affected Service [M.2.1.4.c.i]	[REDACTED] Section 1.4.3.1.
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 [M.2.1.4.c.ii]	[REDACTED] Section 1.4.3.2.
Technical Approach to Notify DHS If Any Non-Participating Agency Traffic Will Be Redirected Through DHS EINSTEIN Enclaves [M.2.1.4.c.iii]	[REDACTED] Section 1.4.3.3.

Requirement	Compliance Description
Control Mechanisms to Ensure the Identification and Redirection of Participating Agency Traffic Cannot Be Inadvertently or Maliciously By-Passed [M.2.1.4.c.iv]	Section 1.4.3.4.
Sensing and Control Mechanisms to Ensure the Redirection of Traffic is Failsafe [M.2.1.4.c.v]	Section 1.4.3.5.
Location of AT&T Certified Facilities [M.2.1.4.c.vi]	Section 1.4.3.6.
Availability of TS/SCI Cleared Personnel for “Smart-Hands” Service of DHS Supplied Equipment [M.2.1.4.c.vii]	Section 1.4.3.7.
Instrumentation to Measure Transport SLA KPIs [M.1.4.c.viii]	Section 1.4.3.8.

2.2.1.5.2 Technical Response for IPS [L.29.2.1; M.2.1]

2.2.1.5.2.1 Service Description and Functional Definition [L.29.2.1; C.2.1.7.1; C.2.1.7.1.1]

Agencies will receive a solution that provides full service scope and functional capabilities, as shown in **Table 2.2.1-29**, and described previously in

Section 2.2.1.5.1.1.

Table 2.2.1-29. IPS Service Scope and Functional Capabilities. Agencies will receive services with the capability to meet service description and functional requirements.

Solution Element	Description
IP protocol transport	<ul style="list-style-type: none"> Provides transport of IP packets via an IP/MPLS network
Protocol suite	<ul style="list-style-type: none"> Supports IPv4 and IPv6 Supports Dual-stack (IPv4/IPv6) IP
Proprietary technology	<ul style="list-style-type: none"> Uses no proprietary technologies in delivery of IPS

2.2.1.5.2.2 Standards [L.29.2.1; C.2.1.7.1.2]

AT&T will comply with all standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.2.1.5.2.3 Connectivity [L.29.2.1; C.2.1.7.1.3]

AT&T will comply with all connectivity instances listed in the RFP as applicable.

2.2.1.5.2.4 Technical Capabilities [L.29.2.1; C.2.1.7.1.4]

All proposed technical capabilities are described in **Table 2.2.1-30** and described previously in **Section 2.2.1.5.1.1**.

Table 2.2.1-30. IPS Technical Capabilities. *The AT&T IP*

#	Technical Capability		Description
1.	Routing requirements		
2.	IPS ports		
3.	Access services		
4.	Network capabilities		
5.	Border gateway protocol		
6.	Routing protocol		

2.2.1.5.2.5 Features [L.29.2.1; C.2.1.7.2]

Agencies will receive an EIS-compliant IPS that meets or exceeds all mandatory features. All proposed features are described in **Table 2.2.1-31**, described previously in **Section 2.2.1.5.1.1**.

Table 2.2.1-31. IPS Features.

Feature		Description
RFP Required Features		
Class of service		

2.2.1.5.2.6 Interfaces [L.29.2.1; C.2.1.7.3]

The AT&T IPS is compatible with interfaces in RFP Section C.2.1.7.3, as applicable.

2.2.1.5.2.7 Performance Metrics [L.29.2.1; C.2.1.7.4]

The AT&T IPS meets all KPIs listed in RFP Section C.2.1.7.4.

2.2.1.6 [REDACTED]



2.2.1.6.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.1.6.1.1 Understanding [L.29.2.1(A); M.2.1(1)]



[REDACTED] **Figure 2.2.1.6-1**
and **Table 2.2.1.6-1** below.

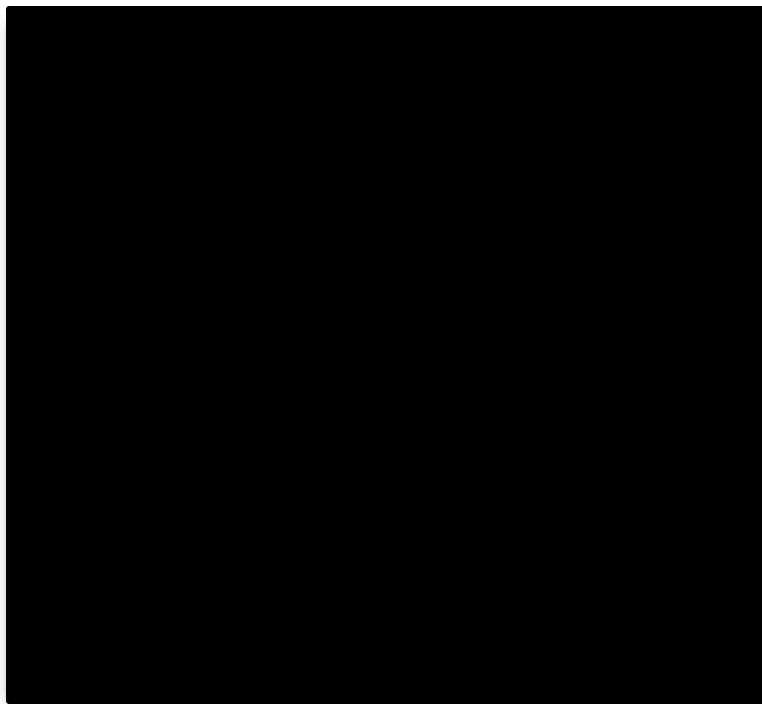





Figure 2.2.1.6-1. BIS Overview. 

Table 2.2.1.6-1. 

Architectural Components	Description
Network Components	
Access loop and termination	<ul style="list-style-type: none">   
Agency Minimum Point of Entry (MPOE)	<ul style="list-style-type: none">             
Service Related Equipment (SRE)	<ul style="list-style-type: none"> 

2.2.1.6.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our [REDACTED] approach and architecture delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.2.1.6-2**.

Table 2.2.1.6-2. BIS Quality of Service. [REDACTED]

Architectural Components	Description
Compliance	
Demonstrated compliance	<ul style="list-style-type: none"> [REDACTED]
Scalability	
IP Passthrough Mode	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Reliability	
Network Transport	<ul style="list-style-type: none"> [REDACTED]
Resilience	
Day 2 Service Assistance	<ul style="list-style-type: none"> [REDACTED]
High Availability	<ul style="list-style-type: none"> [REDACTED]

2.2.1.6.1.3 [REDACTED]

See **Section 1.3** for [REDACTED]

2.2.1.6.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.1.6.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

[REDACTED] C.2.1.8.1.4.1

and are addressed in **Section 2.2.1.6.2.4**. **Table 2.2.1.6-3** delineates additional [REDACTED] service-specific security capabilities delivered to agencies.

Table 2.2.1.6-3. BIS Service-Specific Security Capabilities. [REDACTED]

Capability	Description
Encryption	<ul style="list-style-type: none"> [REDACTED]
Network security	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED]

Capability	Description
	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]

2.2.1.6.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.2.1.6.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3); J.4]

[REDACTED]

Table 2.2.1.6-4 provides detailed references to our approach.

Table 2.2.1.6-4. Approach to External Traffic Routing Requirements.

Requirement	Compliance Description
Methodology for Identifying AT&T Participating Agency Traffic for Each Affected Service [M.2.1.4.c.i].	[REDACTED]
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 [M.2.1.4.c.ii]	[REDACTED]
Technical Approach to Notify DHS If Any Non-Participating Agency Traffic Will Be Redirected Through DHS EINSTEIN Enclaves [M.2.1.4.c.iii]	[REDACTED]
Control Mechanisms to Ensure the Identification and Redirection of Participating Agency Traffic Cannot Be Inadvertently or Maliciously By-Passed [M.2.1.4.c.iv]	[REDACTED]
Sensing and Control Mechanisms to Ensure the Redirection of Traffic is Failsafe [M.2.1.4.c.v]	[REDACTED]
Location of AT&T Certified Facilities [M.2.1.4.c.vi]	[REDACTED]

Requirement	Compliance Description
Availability of TS/SCI Cleared Personnel for “Smart-Hands” Service of DHS Supplied Equipment [M.2.1.4.c.vii]	
Instrumentation to Measure Transport SLA KPIs [M.2.1.4.c.viii]	

2.2.1.6.2 Technical Response for BIS [L.29.2.1; M.2.1]

2.2.1.6.2.1 Service Description and Functional Definition [L.29.2.1; C.2.8.10.1; C.2.8.10.1.1]

Agencies will receive a solution that provides full-service scope and functional capabilities, as described in **Table 2.2.1.6-5** and described previously in **Section 2.2.1.6.1.1**.

Table 2.2.1.6-5. BIS Service Scope and Functional Capabilities.

Solution Element	Description
Network Access	
Embedded Service	
Broadband Speeds	

2.2.1.6.2.2 Standards [L.29.2.1; C.2.8.10.1.2]

AT&T will comply with standards listed in the EIS Contract Section C.2.8.10.1.2, as well as those referenced by the listed standards as applicable.

2.2.1.6.2.3 Connectivity [L.29.2.1; C.2.8.10.1.3]

AT&T will comply with all connectivity instances listed in the EIS Contract Section C.2.8.10.1.3, as applicable.

2.2.1.6.2.4 Technical Capabilities [L.29.2.1; C.2.8.10.1.4]

Table 2.2.1.6-6.

Table 2.2.1.6-6. BIS Technical Capabilities.

#	Technical Capability	Description
1.	Routing requirements per Section C.1.8.8	

#	Technical Capability		Description
2.	Port access components meets or exceeds download bandwidth		
3.	Embedded asymmetric or symmetric access services		
4.	No limit or throttle on data download		
5a.	Established public peering arrangements		
5b.	Private peering arrangements		
5c.	Support government-assigned and InterNIC-registered IP addresses and domain names		
5d.	Primary and secondary DNS	Meets	
5e.	Dynamic or fixed IP addresses	Meets	

2.2.1.6.2.5 Features [L.29.2.1; C.2.8.10.2]

Table 2.2.1.6-7, Section 2.2.1.6.1.1,

Table 2.2.1.6-7. BIS Features.

#	Feature		Description
1.	Enhanced Class of Service (CoS) (Partial)		
2.	Static IP address (Optional)		

2.2.1.6.2.6 Interfaces [L.29.2.1; C.2.8.10.3]

The [REDACTED] Section

C.2.1.8.3, [REDACTED]

2.2.1.6.2.7 Performance Metrics [L.29.2.1; C.2.8.10.4]

The AT&T [REDACTED] Section C.2.1.8.4.

2.2.2 Service Area: Voice Service [C.2.2]

2.2.2.1 Toll Free Service [L.29.2.1; M.2.1; C.2.2.3]

The rapid adoption of mobile communications worldwide is driving changes in the use and configuration of toll free services. [REDACTED]

2.2.2.1.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.2.1.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

AT&T has decades of toll-free service experience, and has been providing full-featured toll-free service since its inception. [REDACTED]

[REDACTED]. Our proposed architecture and TFS services meet EIS service requirements as shown in **Figure 2.2.2-1** and **Table 2.2.2-1**.

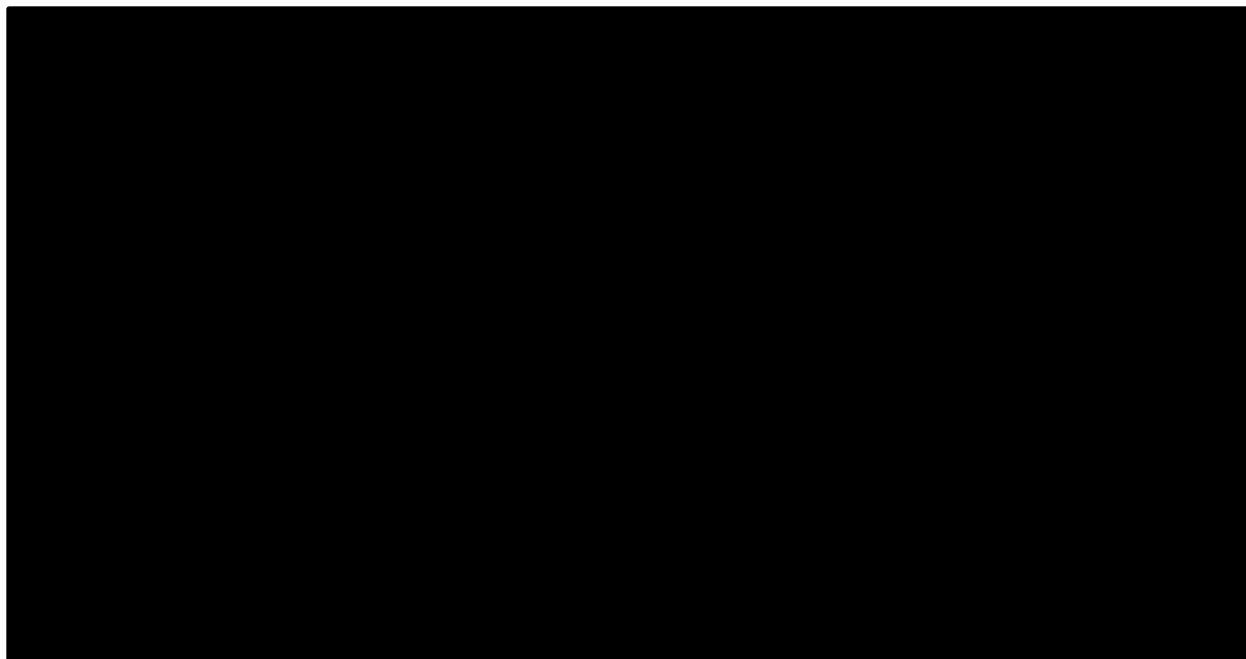


Figure 2.2.2-1. TFS Overview.

Table 2.2.2-1. TFS Overview Description. *We have developed and will deploy a large and fully featured toll-free service infrastructure. Our infrastructure development*

Architectural Components	Description
Functional Components	
Toll free numbers	[Redacted]
Custom call routing	[Redacted]
Announcements	[Redacted]
Call center interaction	[Redacted]
Accounting and reporting	[Redacted]
Physical/Virtual Components	
Toll free call routing	[Redacted]
IVR	[Redacted]
Speech recognition	[Redacted]
IP toll free functions	[Redacted]
Operational Components	

Architectural Components	Description
Toll free number management	
Advanced features	
Toll free routing control	
Toll free network NOC	
IVR management portal	
Network Components	
VoIP network	
SIP trunks	
IP VPN service	
Circuit switched network	
Access	

2.2.2.1.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our TFS approach and architecture delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.2.2-2**.

Table 2.2.2-2. TFS QoS. TFS is fully compliant, and provides the robust scalability, high reliability, and strong resilience sought by GSA and agencies.

Architectural Components	Description
Compliance	
Demonstrated compliance	Section 2.2.2.1.2
Scalability	
Expandable functional blocks	
Very large call centers	
Reliability	
High availability components	
Multiple call processing support	

Architectural Components	Description
Resilience	
Mobile agents and functions	
IP anywhere	

See **Section 1.3** for AT&T service coverage for TFS.

2.2.2.1.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.2.1.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

TFS has no service-specific requirements indicated in the RFP

2.2.2.1.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for TFS are protected from information breaches, unauthorized access and supply chain risks

2.2.2.1.2 Technical Response for TFS [L.29.2.1; M.2.1]

2.2.2.1.2.1 Service Description and Functional Definition [L.29.2.1; C.2.2.3; C.2.2.3.1.1]

Agencies will receive a solution that provides full service scope and functional capabilities, as described in **Table 2.2.2-4**, and described previously in

Section 2.2.2.1.1.1.

Table 2.2.2-4. TFS Service Scope and Functional Capabilities. Agencies will receive services with proven capability to meet service description and functional requirements.

Solution Element	Description
Convenient accessibility	
Range of features	
Proprietary technology	

2.2.2.1.2.2 Standards [L.29.2.1; C.2.2.3.1.2]

AT&T will comply with all standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.2.2.1.2.3 Connectivity [L.29.2.1; C.2.2.3.1.3]

AT&T will comply with all connectivity instances listed in the RFP as applicable.

2.2.2.1.2.4 Technical Capabilities [L.29.2.1; C.2.2.3.1.4]

Agencies will receive a reliable TFS

are described in **Table 2.2.2-5**, and described previously in **Section 2.2.2.1.1.1**.

Table 2.2.2-5. TFS Technical Capabilities. *Agencies will receive services demonstrated to meet required technical capabilities.*

Technical Capability		Description
Toll free numbering		<ul style="list-style-type: none">
Toll free number termination		<ul style="list-style-type: none">
Incomplete calls		<ul style="list-style-type: none">
Network intercept		<ul style="list-style-type: none">
Disconnect referral		<ul style="list-style-type: none">
Dialed number identification service		<ul style="list-style-type: none">
Automatic number identification		<ul style="list-style-type: none">

2.2.2.1.2.5 Features and TFS Feature Reports [L.29.2.1; C.2.2.3.2; C.2.2.3.2.1]

Agencies will receive a reliable TFS that meets all mandatory features, and offers a range of optional features. Proposed features are described in **Table 2.2.2-6**, and described previously in **Section 2.2.2.1.1.1**.

Table 2.2.2-6. TFS Features. Agencies will receive TFS services that are robust and meet the required set of features.

Feature		Description
RFP Required Features		
Agency-based routing (host connect)		<p>Agency-based routing (host connect) is a feature that allows the user to route calls to the appropriate extension based on the host connect number. This feature is required for all agencies.</p>
Cascade routing		<p>Cascade routing is a feature that allows the user to route calls to the appropriate extension based on the cascade number. This feature is required for all agencies.</p>
ANI and ANI-based routing		<p>ANI and ANI-based routing is a feature that allows the user to route calls to the appropriate extension based on the ANI number. This feature is required for all agencies.</p>
Announced connection		<p>Announced connection is a feature that allows the user to route calls to the appropriate extension based on the announced connection number. This feature is required for all agencies.</p>
Announcements		<p>Announcements is a feature that allows the user to route calls to the appropriate extension based on the announcement number. This feature is required for all agencies.</p>
Menu-based routing		<p>Menu-based routing is a feature that allows the user to route calls to the appropriate extension based on the menu-based routing number. This feature is required for all agencies.</p>
Call redirection		<p>Call redirection is a feature that allows the user to route calls to the appropriate extension based on the call redirection number. This feature is required for all agencies.</p>

143

Feature		Description
		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED] • [REDACTED]
Network queuing (optional)		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED] • [REDACTED] • [REDACTED]
NPA/NXX routing		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED] • [REDACTED]
Percentage call allocation		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED]
Real-time reporting		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED] • [REDACTED] • [REDACTED]
Routing control		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED] • [REDACTED] • [REDACTED]
Service assurance routing		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED] • [REDACTED]
Speech recognition		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED] • [REDACTED]
Tailored call coverage		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED] • [REDACTED]
Time of day routing		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED]
Language interpretation service		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED]
Virtual queue		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED]
Vanity toll-free number		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED]

. All proposed features are described in **Table 2.2.2-7**, and described previously in **Section 2.2.2.1.1.1**.

Table 2.2.2-7. TFS Feature Reports. *Agencies receive TFS reports*

Feature		Description
RFP Required Features		
Status of calls reporting		<ul style="list-style-type: none"> ■ [Redacted]
Report transmittal		<ul style="list-style-type: none"> ■ [Redacted] ■ [Redacted] ■ [Redacted]
Reporting time indicators		<ul style="list-style-type: none"> ■ [Redacted] ■ [Redacted]
Standard reporting information		<ul style="list-style-type: none"> ■ [Redacted]
Commercial reporting		<ul style="list-style-type: none"> ■ [Redacted]
Call status report – toll-free service		<ul style="list-style-type: none"> ■ [Redacted]
Call status report – alternate routing		<ul style="list-style-type: none"> ■ [Redacted]
Call status report – announcement		<ul style="list-style-type: none"> ■ [Redacted]
Call status report – call prompter		<ul style="list-style-type: none"> ■ [Redacted]
Call status report – IVR		<ul style="list-style-type: none"> ■ [Redacted]
Caller information report		<ul style="list-style-type: none"> ■ [Redacted]
Caller profile report	Meets	<ul style="list-style-type: none"> ■ We provide caller profile reports for any toll-free number with reports containing items listed on ID Number 7, sub-items 1-5, RFP page 110 for this reporting feature.

Feature		Description
Call redirection report (optional)		

2.2.2.1.2.6 Interfaces [L.29.2.1; C.2.2.3.3]

The AT&T TFS is compatible with interfaces in RFP Section C.2.2.3.3, as applicable.

2.2.2.1.2.7 Performance Metrics [L.29.2.1; C.2.2.3.4]

Section C.2.2.3.4.

2.2.2.2 Circuit Switched Data Service [C.2.2.4-C.2.2.4.4]

CSDS is the evolution of the circuit switching technology from the PSTN's Integrated Service Digital Network (ISDN) initiatives through the 1980s, and is used to reserve dedicated channels (i.e., circuits) for synchronized data transport primarily for video and file transmissions.

2.2.2.2.1 How AT&T Will Provide the Proposed Services and Features [L.29.2.1; M.2.1]

2.2.2.2.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

Figure 2.2.2.2-1 Table 2.2.2.2-1.

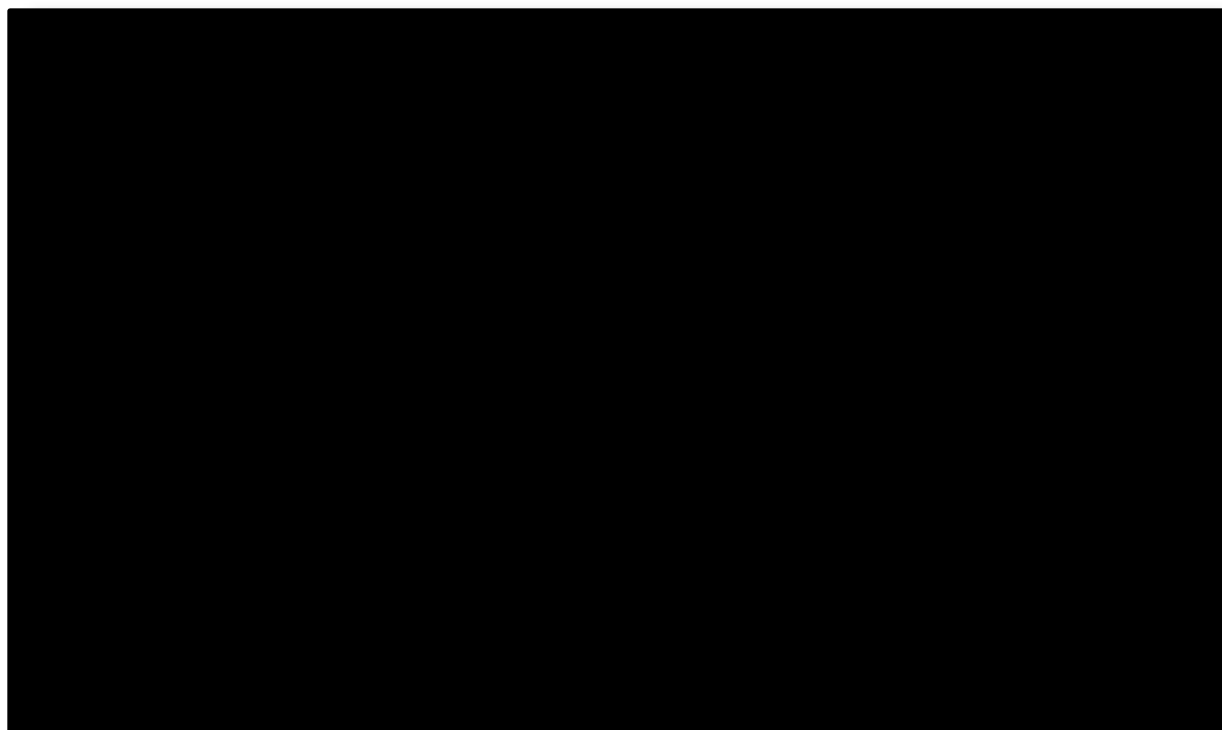


Figure 2.2.2.2-1. CSDS Overview. [Redacted]

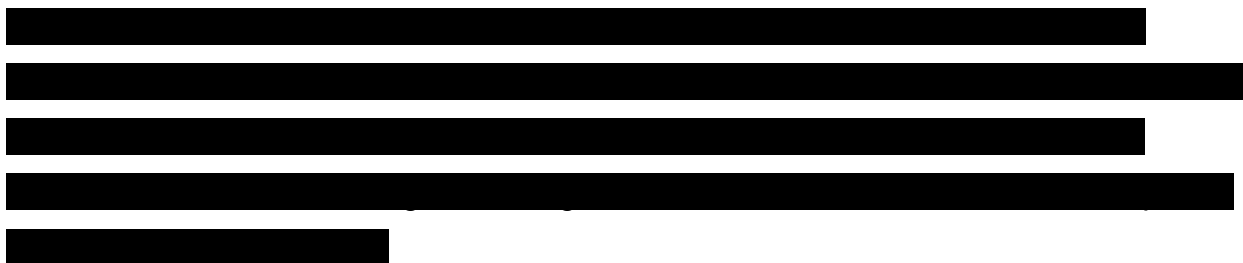


Table 2.2.2.2-1. CSDS Overview Description. [Redacted]

Architectural Components	Description
Functional Components	
5E Switching locations	[Redacted]
4E Switching locations	[Redacted]
SS7	[Redacted]
PIC	[Redacted]
Numbering	[Redacted]



Architectural Components	Description
LNP	<ul style="list-style-type: none"> [REDACTED]
Technical Components	
ISDN PRI	<ul style="list-style-type: none"> [REDACTED]
ISDN BRI	<ul style="list-style-type: none"> [REDACTED]
Operational Components	
AT&T Voice NOC	<ul style="list-style-type: none"> [REDACTED]
PSTN	<ul style="list-style-type: none"> [REDACTED]
Network Components	
5ESS and DMS Switches	<ul style="list-style-type: none"> [REDACTED]
SS7 Signaling and interconnect Network	<ul style="list-style-type: none"> [REDACTED]
Serving Wire Center (SWC)	<ul style="list-style-type: none"> [REDACTED]
Access Circuits	<ul style="list-style-type: none"> [REDACTED]

2.2.2.2.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

[REDACTED]

Table 2.2.2.2-2.

Table 2.2.2.2-2. CSDS Quality of Service.

Architectural Components	Description
Compliance	
Service & Functional Req'ts	<ul style="list-style-type: none"> [REDACTED]
Standards	<ul style="list-style-type: none"> [REDACTED]
Connectivity	<ul style="list-style-type: none"> [REDACTED]
Technical Capabilities	<ul style="list-style-type: none"> [REDACTED]
Features	<ul style="list-style-type: none"> [REDACTED]
Interfaces	<ul style="list-style-type: none"> [REDACTED]
Performance Metrics	<ul style="list-style-type: none"> [REDACTED]
Scalability	
T-Carrier Delivery	<ul style="list-style-type: none"> [REDACTED]

Architectural Components	Description
Reliability	
NEBS Systems Architecture	■ [REDACTED]
SS7 Five-Nines	■ [REDACTED]
Resilience	
Single Circuit Service	■ [REDACTED]

2.2.2.2.1.3 [REDACTED] [L.29.2.1(C); M.2.1(3); C.1.3]

See Section [REDACTED].

2.2.2.2.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.2.2.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]. Table 2.2.2.2-3 [REDACTED]

[REDACTED]

Table 2.2.2.2-3. CSDS Service-Specific Security Capabilities.

Capability	Description
PSTN Based Service	■ [REDACTED]

2.2.2.2.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

[REDACTED] Section 1.4 [REDACTED]

[REDACTED]

2.2.2.2.2 Technical Response for CSDS [L.29.2.1; M.2.1]

2.2.2.2.2.1 Service Description and Functional Definition [L.29.2.1; C.2.2.4.1; C.2.2.4.1.1]

[REDACTED]

[REDACTED] Table 2.2.2.2-4 [REDACTED] Figure 2.2.2.2-1.

Table 2.2.2.2-4. CSDS Service Scope and Functional Capabilities.

Solution Element	Description
Data Calls	■ [REDACTED] ■ [REDACTED]

Solution Element	Description
	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Equipment	<ul style="list-style-type: none"> [REDACTED]
PSTN	<ul style="list-style-type: none"> [REDACTED]

2.2.2.2.2.2 Standards [L.29.2.1; C.2.2.4.1.2; C.1.8.4]

AT&T will comply with all standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.2.2.2.2.3 Connectivity [L.29.2.1; C.2.2.4.1.3]

AT&T will comply with all connectivity instances listed in the RFP as applicable.

2.2.2.2.2.4 Technical Capabilities [L.29.2.1; C.2.2.4.1.4]

[REDACTED]

[REDACTED]

Table 2.2.2.2- [REDACTED] Figure 2.2.2.2-1.

Table 2.2.2.2-5. CSDS Technical Capabilities. Agencies will receive CSDS with proven capability to meet or exceed required technical capabilities.

Technical Capability	[REDACTED]	How Delivered
Uniform numbering plan	[REDACTED]	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Authorization Codes	[REDACTED]	<ul style="list-style-type: none"> [REDACTED]
Bandwidth	[REDACTED]	<ul style="list-style-type: none"> [REDACTED]
Ad Hoc Use	[REDACTED]	<ul style="list-style-type: none"> [REDACTED]
Network Derived Clocking	[REDACTED]	<ul style="list-style-type: none"> [REDACTED]
Data Bit Sequencing	[REDACTED]	<ul style="list-style-type: none"> [REDACTED]
Dialable Payloads	[REDACTED]	<ul style="list-style-type: none"> [REDACTED] [REDACTED]

Technical Capability		How Delivered
		<ul style="list-style-type: none">
Multi-rate Calling		<ul style="list-style-type: none">
Multi-rate DS1 Category (Optional)		
DS3 Category (Optional)		
SONET Level-I Category (Optional)		
SONET Level-II Category (Optional)		
SONET Level-III Category (Optional)		

2.2.2.2.2.5 Features [L.29.2.1; C.2.2.4.2]

Table 2.2.2.2-6 Figure 2.2.2.2-1.

Table 2.2.2.2-6. CSDS Features. Agencies receive CSDS with proven capability to meet or exceed the required set of features.

Feature		How Delivered
Dial-In Capability		<ul style="list-style-type: none">
User-to-User Signaling Via ISDN D-Channel		<ul style="list-style-type: none">
Additional Features		
	n/a	<ul style="list-style-type: none"> No additional features supported

2.2.2.2.2.6 Interfaces [L.29.2.1; C.2.2.4.3]

2.2.2.2.2.7 Performance Metrics [L.29.2.1; C.2.2.4.4; G.8.2]

2.2.3 Service Area: Contact Center Service [C.1.8.1]

2.2.3.1 Contact Center Service [L.29.2.1; M.2.1; C.2.3]

Agencies will receive a reliable, highly secured, and flexible Contact Center Service (CCS). [REDACTED]

2.2.3.1.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.3.1.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

[REDACTED]

[REDACTED] Figure 2.2.3-1 [REDACTED] Table 2.2.3-1.

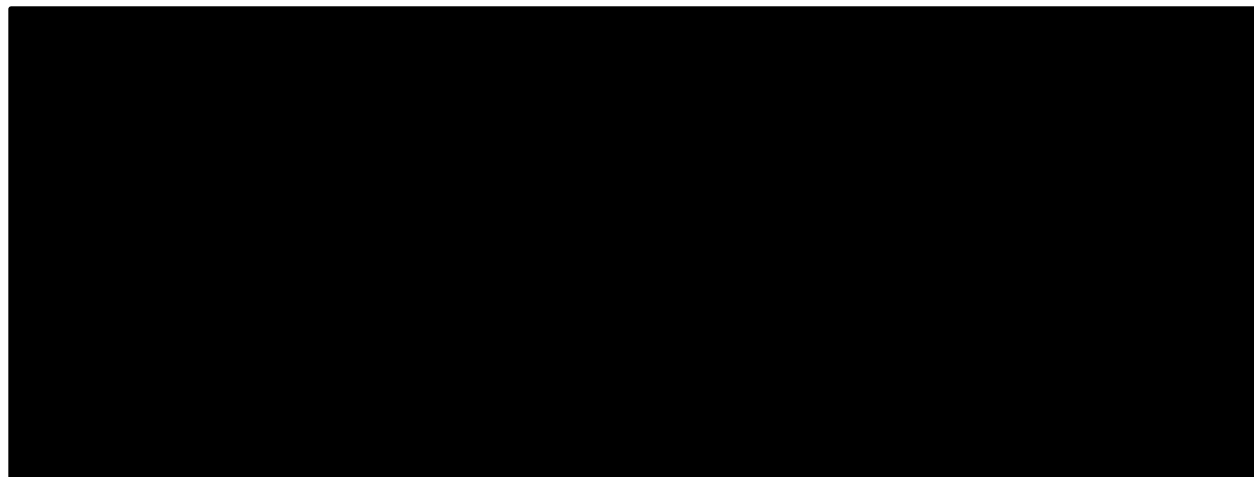


Figure 2.2.3-1. AT&T CCS Solution. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Table 2.2.3-1. AT&Ts CCS Overview Description. Agencies will receive CCS that easily integrates into their current environment, and/or interfaces with other third party providers and outsourcers. CCS, [REDACTED]

Architectural Components	Description
Network Components	
Session border controller	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]

Use or disclosure of data contained on this page is subject to the restriction on the title page of this document.

Architectural Components	Description
	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Speech recognition text to speech	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Intelligent call routing	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Management Components	
Reporting	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED]
System manager	<ul style="list-style-type: none"> [REDACTED] [REDACTED]

2.2.3.1.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our CCS approach and architecture delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.2.3-2**.

Table 2.2.3-2. CCS QoS. Agencies will receive vendor-agnostic CCS customized for each agency's needs.

Architectural Components	Description
Compliance	
Demonstrated compliance	<ul style="list-style-type: none"> [REDACTED]
Scalability	
Expandable size	<ul style="list-style-type: none"> [REDACTED]
Expandable feature set	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Reliability	
Hosted – single	<ul style="list-style-type: none"> [REDACTED]

Architectural Components	Description
Hosted – dual	
Resilience	
Premises based	
Active and host standby software images	

2.2.3.1.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.3.1.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

CCS has no service-specific requirements indicated in the RFP.

2.2.3.1.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for CCS are protected from information breaches, unauthorized access and supply chain risks

2.2.3.1.2 Technical Response for CCS [L.29.2.1; M.2.1]

2.2.3.1.2.1 Service Description and Functional Definition [L.29.2.1; C.2.2.3.1; C.2.2.3.1.1]

Agencies will receive a solution that provides full service, scope, and functional capabilities, as described in **Table 2.2.3-4**, and described previously in

Section 2.2.3.1.1.1.

Table 2.2.3-4. CCS Service Scope and Functional Capabilities. Agencies will receive a fully compliant CCS that supports both IP and TDM.

Solution Element	Description
Customer service delivery	
Network call queue	
Use with other services	
Call answering service	

2.2.3.1.2.2 Standards [L.29.2.1; C.2.2.3.1.2]

AT&T will comply with all applicable standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.2.3.1.2.3 Connectivity [L.29.2.1; C.2.3.1.3]

AT&T will comply with all connectivity instances listed in RFP.

2.2.3.1.2.4 Technical Capabilities [L.29.2.1; C.2.3.1.4-C.2.3.1.4.4]

Agencies will receive leading edge

Table 2.2.3-5

Section 2.2.3.1.1.1.

Table 2.2.3-5. CCS Delivery Methods Technical Capabilities. Agencies will receive

	Technical Capability		Description
CCS Delivery Methods [C.2.3.1.4.1]			
1.	Host-based call management service		
2.	Premises-based call management service		
3.	Premises-based call answering service		
4.	Host-based call answering service		
CCS Call Management Service [C.2.3.1.4.2]			
1.	Network call queue	Meets	
2.	Intelligent call routing	Meets	

	Technical Capability		Description
3.	Interoperability		[REDACTED]
4.	Interoperating with agency security		[REDACTED]
5.	Service observation		[REDACTED]
6.	Managing network queue, call routing, and profile reports		[REDACTED]
7.	Reporting		[REDACTED]
8.	Graphical real-time reporting CCS queue status		[REDACTED]
9.	Queue status reporting		[REDACTED]
10.	Music on hold		[REDACTED]

	Technical Capability		Description
11.	Terminal devices		<ul style="list-style-type: none"> [REDACTED] [REDACTED]
12.	Contact center closing/announcements		<ul style="list-style-type: none"> [REDACTED]
CCS Call Answering Service [C.2.3.1.4.3; C.2.3.1.4.4]			
1.	Contact center operation		<ul style="list-style-type: none"> [REDACTED] [REDACTED]
2.	Call answering service		<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
3.	CCS resources		<ul style="list-style-type: none"> [REDACTED]
CCS Call Answering Resources Table [C.2.3.1.4.4]			
1.	Basic call answering		<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

2.2.3.1.2.5 Features [L.29.2.1; C.2.3.1.5]

Agencies will receive established [REDACTED]. All proposed features are described in **Table 2.2.3-6**, and described previously in **Section 2.2.3.1.1.1**.

#	Feature		Description
RFP Required Features			
1.	Call recording and monitoring		[Redacted]
2.	Collaborative browsing		[Redacted]
3.	Computer telephony integration		[Redacted]
4.	Customer contact application		[Redacted]

Use or disclosure of data contained on this page is subject to the restriction on the title page of this document.

#	Feature		Description
13.	Web call back	Meets	
14.	Web call through	Meets	
15.	Workforce management	Meets	
16.	Virtual queue	Meets	

2.2.3.1.2.6 Interfaces [L.29.2.1; C.2.3.1.6]

AT&T CCS is compatible with the interfaces referenced in RFP Section C.2.3.1.6, as applicable.

2.2.3.1.2.7 Performance Metrics [L.29.2.1; C.2.3.1.7]

The AT&T CCS meets all KPIs listed in RFP Section C.2.3.1.7.

2.2.4 Service Area: Colocated Hosting Service [C.2.4]

2.2.4.1 Data Center Service/Colocated Hosting Service [L.29.2.1; M.2.1; C.1.8.1; C.2.4]

Agencies will receive a reliable, highly secured, scalable, and globally available Colocated Hosting Service (CHS), also referred to as Data Center Service in RFP Section C.1.8.1, offering connectivity to a high-availability IP-backbone

Industry Accolades for AT&T CHS

network, and an extensive hosting service portfolio, [REDACTED]

2.2.4.1.1 How AT&T Will Provide Proposed Services and Features

[L.29.2.1; M.2.1]

2.2.4.1.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

The proposed AT&T CHS solution will enable agencies to secure their own equipment in racks and cages within an AT&T IDC. [REDACTED]

[REDACTED] CHS also interconnects to the AT&T highly available IP backbone via high-speed connections and provides global connectivity [REDACTED]

The AT&T proposed architecture and [REDACTED]

■ **Figure 2.2.4-1 and Table 2.2.4-1.**

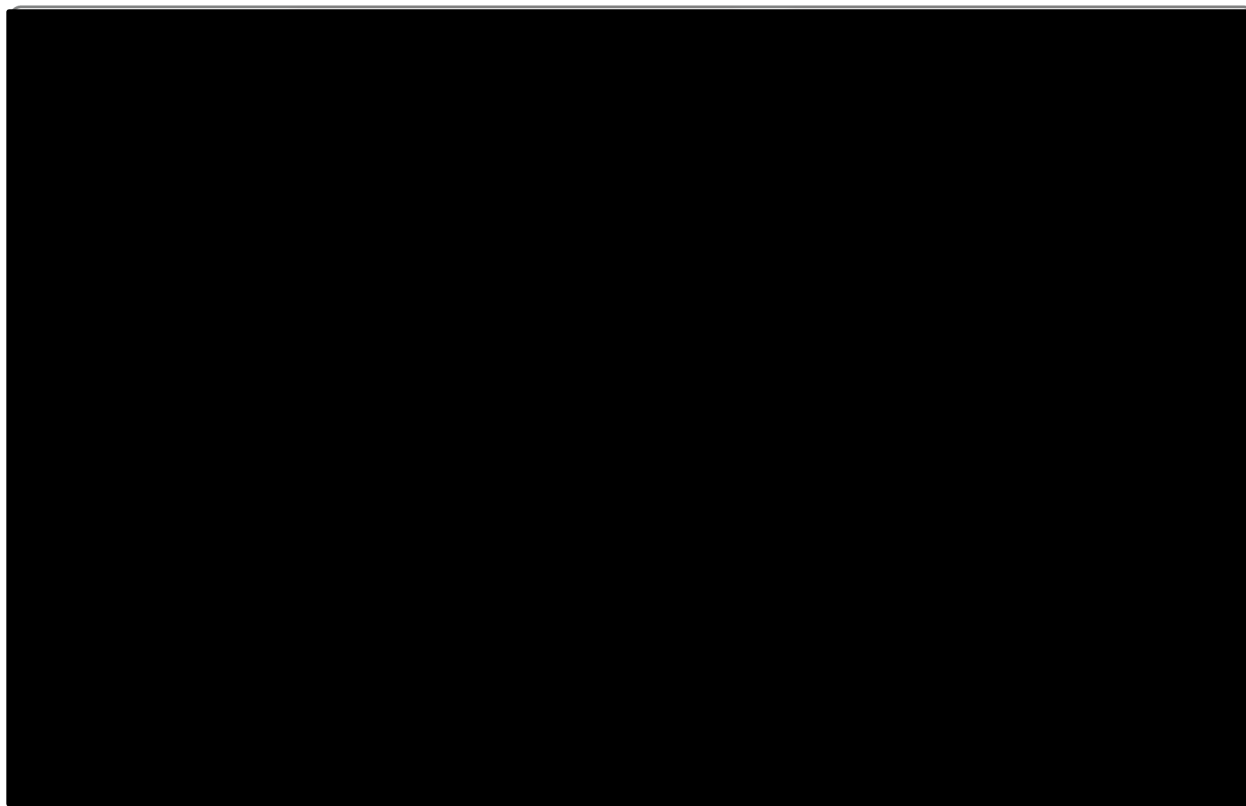


Figure 2.2.4-1. CHS Overview. [REDACTED]

Table 2.2.4-1. CHS Overview Description.

Architectural Components	Description
Functional Components	
Functional definition	<ul style="list-style-type: none"> Functional definition Functional definition Functional definition
CHS facility access	CHS facility access
CHS facility utility infrastructure	<ul style="list-style-type: none"> CHS facility utility infrastructure CHS facility utility infrastructure CHS facility utility infrastructure CHS facility utility infrastructure CHS facility utility infrastructure <p>Table 2.2.4-4</p> <p>Table 2.2.4-4</p>
Technical Components	
Comprehensive physical security measures	Comprehensive physical security measures
Logical security	Logical security
Operational Components	
Hosting infrastructure monitoring and management	Hosting infrastructure monitoring and management
Network Components	
Connectivity to tier 1 internet service providers	Connectivity to tier 1 internet service providers

2.2.4.1.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our CHS approach and architecture delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.2.4-2**.

Table 2.2.4-2. CHS QoS. CHS is fully compliant, and provides the robust scalability, high reliability, and strong resilience sought by GSA and agencies. Service quality

Architectural Components	Description
Compliance	
Demonstrated compliance	<ul style="list-style-type: none"> Demonstrated compliance <p>Section 2.2.4.1.2.4</p>
Scalability	
Meeting demand for growth	Meeting demand for growth
Service flexibility	Service flexibility

Architectural Components	Description
Reliability	
Performance metrics	■ [REDACTED] Section C.2.4.5.1,
Network availability	■ [REDACTED] Section C.2.4.5.1
Resilience	
IDC architecture	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ Figure 2.2.4-2, [REDACTED] ■ [REDACTED] ■ [REDACTED]

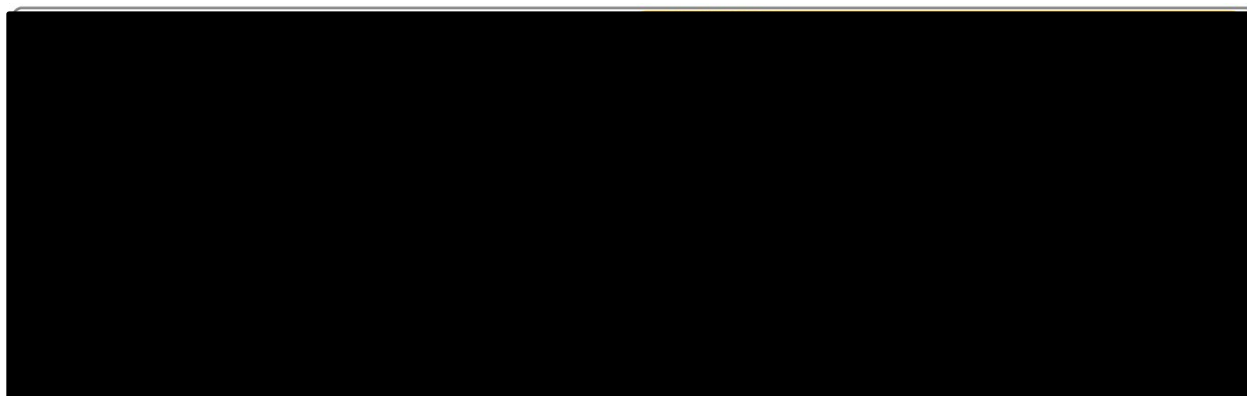


Figure 2.2.4-2. IDC Architecture. [REDACTED]

2.2.4.1.1.3 [REDACTED]

CHS is not a CBSA-dependent service.

2.2.4.1.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.4.1.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

CHS has no service-specific requirements indicated in the RFP.

2.2.4.1.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for CHS are protected from information breaches, unauthorized access and supply chain risks [REDACTED]

[REDACTED]

2.2.4.1.2 Technical Response for DCS/CHS [L.29.2.1; M.2.1]

2.2.4.1.2.1 Service Description and Functional Definition [L.29.2.1; C.2.4.1]

Agencies will receive a solution that provides full service scope and functional capabilities, as described in **Table 2.2.4-4**, and described previously in **Section 2.2.4.1.1.1**.

Table 2.2.4-4. CHS Service Scope and Functional Capabilities. Agencies will receive services

#	Solution Element	Description
1.	Functional definition	<ul style="list-style-type: none"> Provides agencies with a secured location for their GFP, including cages and racks, and site surveillance Defines the following through agency TOs: <ul style="list-style-type: none"> Internet and other dedicated connection speeds, including: PLS, ETS, and total service Plain Old Telephone service (POTS) Cross-connect cabling, including copper, coax, and fiber Space requirements Maintenance and operational support: agencies short on staff can allow on-site AT&T technicians to perform tasks on agency GFP, including periodic hardware check (PING), host administrative tasks (Remote Hands), and/or storage media changes Operates and staffs all IDCs with a security guard 24x7, allowing agency personnel 24x7 access to leased space and GFP
2.	Redundant and highly available power to GFP	
3.	Redundant uninterruptible power supplies	
4.	Smoke detection	
5.	Fire suppression	

#	Solution Element	Description
6.	Cooling and ventilation	

2.2.4.1.2.2 Standards [L.29.2.1; C.2.4.2]

AT&T will comply with all standards listed in the RFP including those listed above and with other standards referenced by the listed standards as applicable.

2.2.4.1.2.3 Connectivity [L.29.2.1; C.2.4.3]

AT&T will provide external connectivity as required in accordance with the TO.

2.2.4.1.2.4 Technical Capabilities [L.29.2.1; C.2.4.4]

Agencies will receive CHS that meets all mandatory technical capabilities. All proposed technical capabilities are described in **Table 2.2.4-5**, and described previously in

Section 2.2.4.1.1.1.

Table 2.2.4-5. CHS Technical Capabilities.

#	Technical Capability		Description
1.	a) Damage or injury to persons or property		
	b) Pre-delivery preparations		
	c) GFP relocation		
	d) Final installation site preparation		
	e) Facilitate GFP setup		
	f) Contractor personnel requirements		
2.	Authorized access to GFP		

#	Technical Capability		Description
3.	Facility and equipment remote monitoring		
4.	Facility and communication error alarms		
5.	Colocated hosting space status and logs		

2.2.4.1.2.5 Features [L.29.2.1; C.2.4.5]

Agencies will receive CHS that meets all mandatory features. All proposed features are described in **Table 2.2.4-6**, and described previously in **Section 2.2.4.1.1.1**.

Table 2.2.4-6. CHS Features. Agencies will services that meet the required feature. Our proposed feature is available in secured CHS facilities with an additional government-only facility currently under construction.

Feature	Meets or Exceeds	Description
RFP Required Features		
Provide CHS in an ICD 705 SCIF	Meets	<ul style="list-style-type: none"> ■ Uses AT&T technical architects to design and assist in the buildout of secured CHS space in a SCIF based on specific requirements defined in an agency TO ■ Works with agency representatives to certify the CHS SCIF space to ICD 705 and any additional agency directives

2.2.4.1.2.6 Interfaces [L.29.2.1]

The RFP identifies no required interfaces for CHS.

2.2.4.1.2.7 Performance Metrics [L.29.2.1; C.2.4.5.1]

The AT&T CHS meets all KPIs listed in RFP Section C.2.4.5.1.

2.2.5 Service Area: Cloud Service [C.2.5]

Agencies will benefit from AT&T Cloud Services that rapidly respond to changing business and operational requirements with accredited cloud services that allow federal IT organizations to meet mandates, drive efficiencies, and increase innovation for mission-critical applications.

Coupled with the AT&T network platform, we deliver an ecosystem of CSP offerings to the

Table 2.2.5-1

Table 2.2.5-1. Cloud Essential Characteristics. *Cloud services in the AT&T ecosystem offer essential features.*

Essential Characteristic	Description
On-demand self service	[REDACTED]
Broad network access	[REDACTED]
Location independent resource pooling	[REDACTED]
Rapid elasticity	[REDACTED]
Measured service	[REDACTED]
Security	[REDACTED]

Figure 2.2.5-1 [REDACTED]

[REDACTED]. In both our current offer and future offers, we will provide the government with an end-to-end solution to integrate new cloud services with existing technology, including highly secured network connectivity, for a smooth and efficient transition to the cloud.

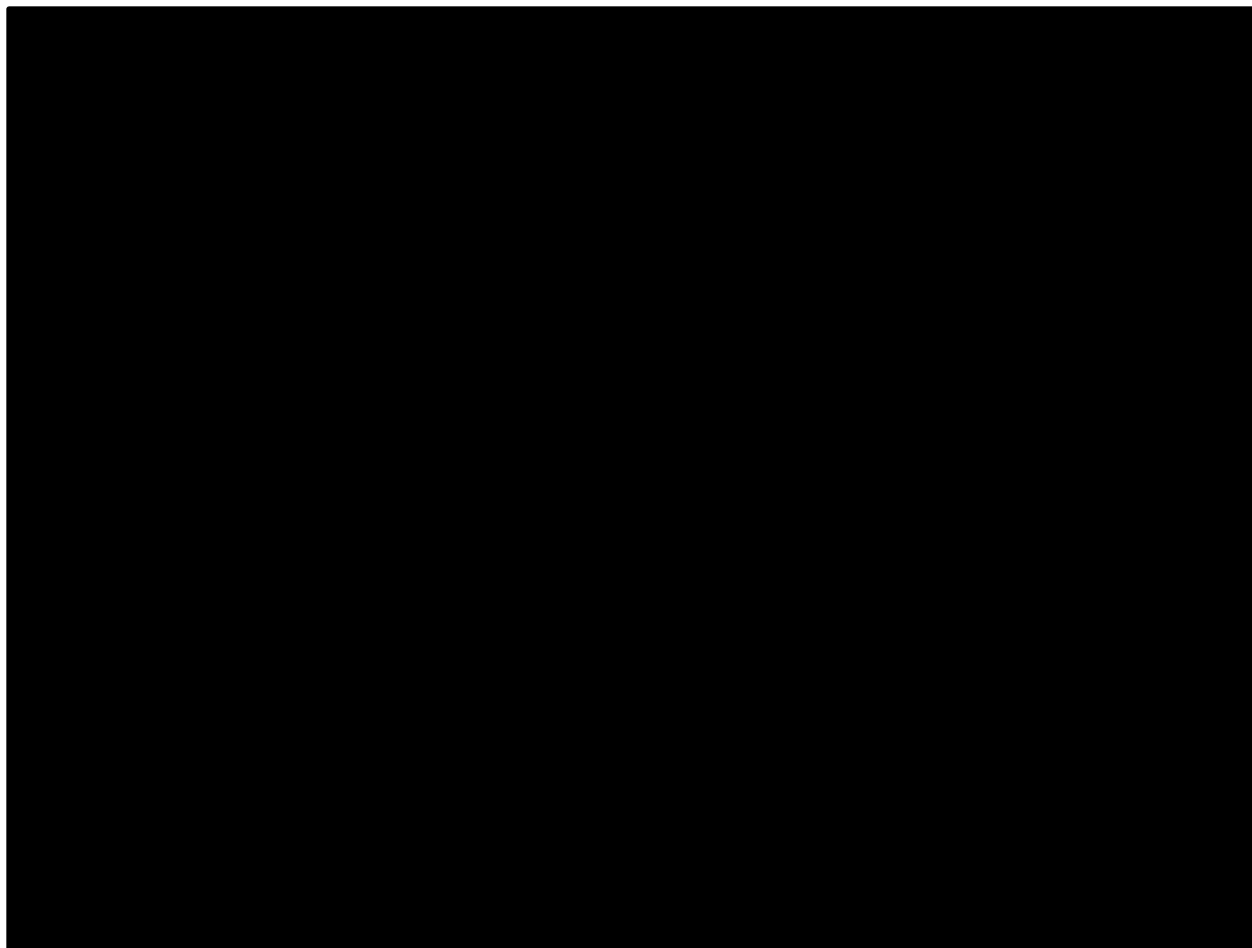


Figure 2.2.5-1. AT&T Current and Future Portfolio of Cloud Services Enables Transition to Cloud for Varying IT Needs.

Agencies may elect to use, for an additional charge, our innovative capability to connect to any cloud service in the AT&T ecosystem through the AT&T NetBond® service, a

[Redacted text block consisting of five lines of blacked-out content]

2.2.5.1 Infrastructure as a Service [L.29.2.1; M.2.1; C.2.5.1]

[REDACTED]



2.2.5.1.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.5.1.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

[REDACTED]

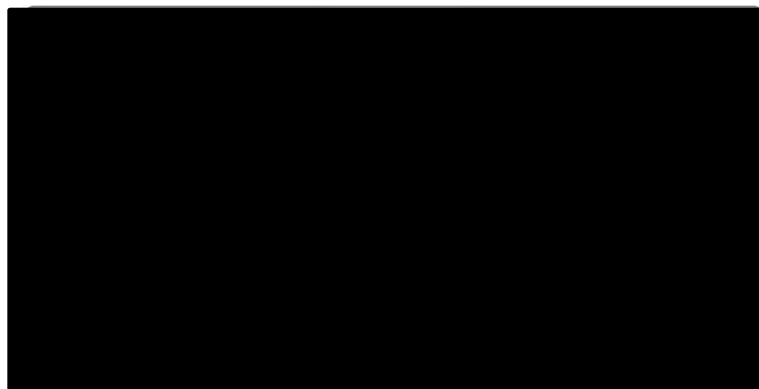


Figure 2.2.5-2 and in
Table 2.2.5-2.

Figure 2.2.5-2. Cloud Services Security.

Table 2.2.5-2. IaaS Overview Description.

Architectural Components	Cloud Services
IaaS	
Private cloud and network storage	[REDACTED]
Backup	[REDACTED]
Disaster recovery/continuity of operations	[REDACTED]

2.2.5.1.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Table 2.2.5-3.

Architectural Components	Description
Compliance	
Demonstrated compliance	<ul style="list-style-type: none"> Section 2.2.5.1.2
Scalability	
Capacity management	<ul style="list-style-type: none">
On-demand resources	<ul style="list-style-type: none">
Automation	<ul style="list-style-type: none">
Reliability	
Infrastructure design	<ul style="list-style-type: none">
Automation	<ul style="list-style-type: none">

Architectural Components	Description
Resilience	
Infrastructure design	
Monitoring	
Flexibility	

2.2.5.1.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.5.1.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

Section 2.2.5.1.2.4. , Figure 2.2.5-2

Table 2.2.5-4

Table 2.2.5-4. Cloud Services Service-Specific Security Capabilities.

Capability	Description
Encryption	
Network security	
Application security	
Third-party validation	

2.2.5.1.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

2.2.5.1.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3)]

Table 2.2.5-5

Table 2.2.5-5. Approach to External Traffic Routing Requirements.

Requirement	Compliance Description
Methodology for Identifying AT&T Participating Agency Traffic for Each Affected Service [M.2.1.4.c.i]	Section 1.4.3.1.
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 [M.2.1.4.c.ii]	Section 1.4.3.2.
Technical Approach to Notify DHS If Any Non-Participating Agency Traffic Will Be Redirected Through DHS EINSTEIN Enclaves [M.2.1.4.c.iii]	Section 1.4.3.3.
Control Mechanisms to Ensure the Identification and Redirection of Participating Agency Traffic Cannot Be Inadvertently or Maliciously By-Passed [M.2.1.4.c.iv]	Section 1.4.3.4.
Sensing and Control Mechanisms to Ensure the Redirection of Traffic is Failsafe [M.2.1.4.c.v]	Section 1.4.3.5.
Location of AT&T Certified Facilities [M.2.1.4.c.vi]	Section 1.4.3.6.
Availability of TS/SCI Cleared Personnel for “Smart-Hands” Service of DHS Supplied Equipment [M.2.1.4.c.vii]	Section 1.4.3.7.
Instrumentation to Measure Transport SLA KPIs [M.2.1.4.c.viii]	Section 1.4.3.8.

2.2.5.1.2 Technical Response for IaaS [L.29.2.1; M.2.1]

2.2.5.1.2.1 Service Description and Functional Definition [L.29.2.1; C.2.5.1.1; C.2.5.1.1.1]

Table 2.2.5-6,

Section 2.2.5.1.1.1.

Table 2.2.5-6. IaaS Service Scope and Functional Capabilities.

Solution Element	Description
Provisioning	
FedRAMP compliance	
Private cloud IaaS	
Data center augmentation with common IT service management	

2.2.5.1.2.2 Standards [L.29.2.1; C.2.5.1.1.2]

2.2.5.1.2.3 Connectivity [L.29.2.1; C.2.5.1.1.3]

2.2.5.1.2.4 Technical Capabilities [L.29.2.1; C.2.5.1.1.4; C.2.5.1.1.4.1; C.2.5.1.1.4.2]

Table 2.2.5-7

Section 2.2.5.1.1.1.

Table 2.2.5-7. IaaS Technical Capabilities

#	Capability	Description
Technical Capabilities of Private Cloud [C.2.5.1.1.4.1]		
1.	Access	
2.	Cloud data center security	
3.	Agency cloud service security	
4.	Virtualized elastic	

#	Capability		Description
	computing infrastructure		
5.	Server hosting		
6.	Backup and restore agency data		
7.	Portal and API		
8.	Usage control and reporting		
9.	User VMs		
10.	Portability		
11.	Access		
12.	Metadata tags (optional)		
13.	Cost control measures		
14.	Customer service		
15.	Exclusive data ownership		
16.	Resource location		
17.	Disaster recovery/continuity of operations		
Technical Capabilities of Data Center Augmentation with Common Information Technology Service Management [C.2.5.1.1.4.2]			
1-3	ITSM		

#	Capability		Description
	Proprietary technology		

2.2.5.1.2.5 Features [L.29.2.1; C.2.5.1.2]

Table 2.2.5-8,

Section 2.2.5.1.1.1.

Table 2.2.5-8. IaaS Features. Agencies will receive services that meet or exceed the required set of features.

Feature		Description
Data management and analytics		
Bare metal servers (optional)		

2.2.5.1.2.6 Interfaces [L.29.2.1; C.2.5.1.3]

.

2.2.5.1.2.7 Performance Metrics [L.29.2.1; C.2.5.1.4]

.

2.2.5.2 Platform as a Service [L.29.2.1; M.2.1; C.2.5.2]

.

2.2.5.2.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.5.2.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

Table 2.2.5.2-1

Table 2.2.5.2-1. PaaS Overview Description

Architectural Components	Description
Developer Tools	
Integrated development environment	
Application server	
Utilities/Libraries	
Database Systems	
DBMS/RDBMS	
Big Data Solutions	
Big data platform	
Directory Services	
Directory services	
Testing Tools	
Application and web testing	
Workflow	

2.2.5.2.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Table 2.2.5.2-2.

Table 2.2.5.2-2. PaaS Quality of Service.

Architectural Components	Description
Compliance	
Demonstrated compliance	

		Section 2.2.5.2.2,	
Scalability			
Capacity management			
On-demand resources			
Automation			
Reliability			
Infrastructure design			
Automation			
Resilience			
Infrastructure design			
Monitoring			
Automation			

2.2.5.2.1.3 Service Coverage (CBSA-Dependent) [L.29.2.1(C); M.2.1(3); C.1.3]

2.2.5.2.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.5.2.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

Section 2.2.5.1.2.4. , Figure 2.2.5-2

Table 2.2.5.2-3

Table 2.2.5.2-3. Cloud Services Service-Specific Security Capabilities.

Capability	Description		
Encryption			
Network security			

Capability	Description
Application security	
Third-party validation	

2.2.5.2.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

Section 1.4 of the Technical Volume.

2.2.5.2.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3); J.4]

Table 2.2.5.2-4

Table 2.2.5.2-4. Approach to External Traffic Routing Requirements.

Requirement	Compliance Description
Methodology for Identifying AT&T Participating Agency Traffic for Each Affected Service [M.2.1.4.c.i].	Section 1.4.3.1
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 [M.2.1.4.c.ii]	Section 1.4.3.2
Technical Approach to Notify DHS If Any Non-Participating Agency Traffic Will Be Redirected Through DHS EINSTEIN Enclaves [M.2.1.4.c.iii]	Section 1.4.3.3
Control Mechanisms to Ensure the Identification and Redirection of Participating Agency Traffic Cannot Be Inadvertently or Maliciously By-Passed [M.2.1.4.c.iv]	Section 1.4.3.4

Requirement	Compliance Description
Sensing and Control Mechanisms to Ensure the Redirection of Traffic is Failsafe [M.2.1.4.c.v]	Section 1.4.3.5
Location of AT&T Certified Facilities [M.2.1.4.c.vi]	Section 1.4.3.6
Availability of TS/SCI Cleared Personnel for “Smart-Hands” Service of DHS Supplied Equipment [M.2.1.4.c.vii]	Section 1.4.3.7
Instrumentation to Measure Transport SLA KPIs [M.2.1.4.c.viii]	Section 1.4.3.8

2.2.5.2.2 Technical Response for PaaS [L.29.2.1; M.2.1]

2.2.5.2.2.1 Service Description and Functional Definition [L.29.2.1; C.2.5.2.1; C.2.5.2.1.1]

[REDACTED]

Table 2.2.5.2-5 [REDACTED] Section 2.2.5.2.1.1.

Table 2.2.5.2-5. PaaS Service Scope and Functional Capabilities. [REDACTED]

Solution Element	Description
Create, deploy, and manage applications in the cloud	[REDACTED]
Proprietary technology	[REDACTED]

2.2.5.2.2.2 Standards [L.29.2.1; C.2.5.2.1.2]

[REDACTED] the RFP and with other standards referenced by the listed standards as applicable.

2.2.5.2.2.3 Connectivity [L.29.2.1; C.2.5.2.1.3]

[REDACTED]

2.2.5.2.2.4 Technical Capabilities [L.29.2.1; C.2.5.2.1.4]

[REDACTED]

Table 2.2.5.2-6.

Table 2.2.5.2-6. PaaS Technical Capabilities.

Technical Capability		Description
Access		
Developer tools:		
▪ IDE suite		
▪ Application server		
▪ Utilities/Libraries		
Database systems		
Big data solutions		
Directory services		
Application and web testing tools		
Workflow tools		

2.2.5.2.2.5 Features [L.29.2.1; C.2.5.2.2]

2.2.5.2.2.6 Interfaces [L.29.2.1; C.2.5.2.3]

2.2.5.2.2.7 Performance Metrics [L.29.2.1; C.2.5.2.4]

Section C.2.5.2.4.

2.2.5.3 Software as a Service [L.29.2.1; M.2.1; C.2.5.3]

2.2.5.3.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.5.3.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Table 2.2.5.3-1 [REDACTED].

Table 2.2.5.3-1. SaaS Overview Description. [REDACTED]

[REDACTED]	[REDACTED]
Customer relationship management	[REDACTED]
Enterprise resource planning	[REDACTED]
Human capital management (HCM)	[REDACTED]
Desktop applications	[REDACTED]
Office automation	[REDACTED]
Architectural Components	Description
Security Tools	<ul style="list-style-type: none"> [REDACTED]

2.2.5.3.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Table 2.2.5.3-2.

Table 2.2.5.3-2. SaaS Quality of Service.

Architectural Components	Description
Compliance	
Demonstrated compliance	<ul style="list-style-type: none"> Section 2.2.5.3.2
Scalability	
Capacity management	
On-demand resources	
Automation	
Reliability	
Infrastructure design	
Automation	
Resilience	
Infrastructure design	
Monitoring	
Automation	

2.2.5.3.1.3

2.2.5.3.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.5.3.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

Section 2.2.5.1.2.4. , Figure 2.2.5-2

Table 2.2.5.3-3,

Table 2.2.5.3-3. Cloud Services Service-Specific Security Capabilities.

Capability	Description
Encryption	
Network security	
Application security	
Third-party validation	

2.2.5.3.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

Section 1.4 of the Technical Volume.

2.2.5.3.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3); J.4]

Table 2.2.5.3-4

Table 2.2.5.3-4. Approach to External Traffic Routing Requirements.

Requirement	Compliance Description
Methodology for Identifying AT&T Participating Agency Traffic for Each Affected Service [M.2.1.4.c.i].	Section 1.4.3.1
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 [M.2.1.4.c.ii]	Section 1.4.3.2
Technical Approach to Notify DHS If Any Non-Participating Agency Traffic Will Be Redirected Through DHS EINSTEIN Enclaves [M.2.1.4.c.iii]	Section 1.4.3.3
Control Mechanisms to Ensure the Identification and Redirection of Participating Agency Traffic Cannot Be Inadvertently or Maliciously By-Passed [M.2.1.4.c.iv]	Section 1.4.3.4

Requirement	Compliance Description
Sensing and Control Mechanisms to Ensure the Redirection of Traffic is Failsafe [M.2.1.4.c.v]	Section 1.4.3.5
Location of AT&T Certified Facilities [M.2.1.4.c.vi]	Section 1.4.3.6
Availability of TS/SCI Cleared Personnel for “Smart-Hands” Service of DHS Supplied Equipment [M.2.1.4.c.vii]	Section 1.4.3.7
Instrumentation to Measure Transport SLA KPIs [M.2.1.4.c.viii]	Section 1.4.3.8

2.2.5.3.2 Technical Response for SaaS [L.29.2.1; M.2.1]

2.2.5.3.2.1 Service Description and Functional Definition [L.29.2.1; C.2.5.3.1; C.2.5.3.1.1]

Table 2.2.5.3-5, Section

2.2.5.3.1.1.

Table 2.2.5.3-5. SaaS Service Scope and Functional Capabilities.

Solution Element	Description
Software as a service	
Proprietary technology	

2.2.5.3.2.2 Standards [L.29.2.1; C.2.5.3.1.2]

2.2.5.3.2.3 Connectivity [L.29.2.1; C.2.5.3.1.3]

2.2.5.3.2.4 Technical Capabilities [L.29.2.1; C.2.5.3.1.4]

Table 2.2.5.3-6.

Table 2.2.5.3-6. SaaS Technical Capabilities.

#	Technical Capability		Description
1.	Compliance with national policy requirements		
2.	CRM Tools		
3.	ERP Tools		
4.	HCM Tools		
5.	Desktop applications		
6.	Office automation tools		
7.	Security tools		
8.	Other/Data access tools		

2.2.5.3.2.5 Features [L.29.2.1; C.2.5.3.2]

2.2.5.3.2.6 Interfaces [L.29.2.1; C.2.5.3.3]

2.2.5.3.2.7 Performance Metrics [L.29.2.1; C.2.5.3.4]

2.2.5.4 Content Delivery Network Service [L.29.2.1; M.2.1; C.2.5.4]

Agencies will give users a dynamic, responsive experience by leveraging features of the AT&T Content Delivery Network Service (CDNS)

2.2.5.4.1 *How AT&T Will Provide Proposed Services and Features* [L.29.2.1; M.2.1]

2.2.5.4.1.1 *Understanding [L.29.2.1(A); M.2.1(1)]*

Agencies will receive a scalable, globally available CDNS that will meet the requirements of this solicitation. Our CDNS provides agencies with a highly available static content download service and streaming,

Figure 2.2.5-3 and Table 2.2.5-9.

Figure 2.2.5-3. CDNS Overview.

Table 2.2.5-9. CDNS Overview Description.

Architectural Components	Description
Functional Components	
Functional definition	<ul style="list-style-type: none">
Technical and operational stipulations	<ul style="list-style-type: none"> Table 2.2.5-12.
Technical Components	
Content delivery capabilities	<ul style="list-style-type: none">

2.2.5.4.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Table 2.2.5-10. CDNS QoS. *Our CDNS is fully compliant, and provides the robust scalability, high reliability, and strong resilience sought by agencies.*

Use or disclosure of data contained on this page is subject to the restriction on the title page of this document.

Architectural Components	Description
Redirection and distribution service (load balancing)	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]

CDNS is not a [REDACTED]-dependent service.

2.2.5.4.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.5.4.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

CNA has no service-specific requirements indicated in the RFP.

2.2.5.4.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for CDNS are protected from information breaches, unauthorized access and supply chain risks [REDACTED]

2.2.5.4.2 Technical Response for CDNS [L.29.2.1; M.2.1]

2.2.5.4.2.1 Service Description and Functional Definition [L.29.2.1; C.2.5.4.1; C.2.5.4.1.1]

Agencies will receive a solution that provides full service scope and functional capabilities, as described in **Table 2.2.5-12**, and described previously in

Section 2.2.5.4.1.1.

Table 2.2.5-12. CDNS Service Scope and Functional Capabilities. Agencies will receive service that meet service description and functional requirements.

Solution Element	Description
CDNS functional definition	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
CDNS technical and operational stipulations	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]

Solution Element	Description

2.2.5.4.2.2 Standards [L.29.2.1; C.2.5.4.1.2]

AT&T will comply with all relevant standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.2.5.4.2.3 Connectivity [L.29.2.1; C.2.5.4.1.3]

AT&T will comply with all connectivity instances listed in the RFP as applicable.

2.2.5.4.2.4 Technical Capabilities [L.29.2.1; C.2.5.4.1.4]

Agencies will receive CDNS

Table 2.2.5-13,

Section 2.2.5.4.1.1.

Table 2.2.5-13. CDNS Technical Capabilities.

#	Technical Capability		Description
1. 1.a) i.	Content distribution – static content download service		
1. b) i.	Real-time streaming (webcasting)		
1. b) ii.	Real-time streaming platforms		
1. c) i.	On-demand streaming		
1. c) ii.	On-demand streaming platforms		
2. a)	Site monitoring/ Origin server performance measurements		

#	Technical Capability		Description
2. b)	Performance dashboard		

CDNS Suite of Services: Agencies can subscribe to any or all CDNS services, as further described in **Table 2.2.5-14**, to meet their specific requirements.

Table 2.2.5-14. CDNS Technical Capabilities. Agencies can subscribe to the CDNS solution suite of services in service bundles or independently, which provides value-added features to the standard CDN service.

Solution Element	Description

2.2.5.4.2.5 Features [L.29.2.1; C.2.5.4.2]

Agencies will receive a

Table 2.2.5-15.

Table 2.2.5-15. CDNS Features.

Feature		Description
RFP Required Features		
Failover service		
(Optional) Redirection and distribution service (global load balancing)		

2.2.5.4.2.6 Interfaces [L.29.2.1; C.2.5.4.3]

The AT&T CDNS is compatible with interfaces in RFP Section C.2.5.4.3, as applicable.

2.2.5.4.2.7 Performance Metrics [L.29.2.1; C.2.5.4.4; C.2.5.4.4.1]

The AT&T CDNS meets all KPIs listed in RFP Section C.2.5.4.4.1.

2.2.6 Service Area: Wireless Service [C.1.8.1]

2.2.6.1 Wireless Service [L.29.2.1; M.2.1; C.2.6]

Agencies will be able to access the AT&T mobility network, which delivers Mobile Wireless Services (MWS), including mobile voice, data, and video services with excellent quality at unprecedented speeds in a broad service area. AT&T continues

to advance and expand our network today, providing new mobile applications that will help agency employees and assets access the network in new ways and places to deliver on mission objectives.

2.2.6.1.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.6.1.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

Agencies will receive flexibility over both service plans and devices with the broad range of options for varying mobile applications, offering options for: voice, push to talk (PTT), voice/data, and data only; an appropriate plan is available for every agency mission requiring mobility.

AT&T MWS Experience	
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]
■	[REDACTED]

Figure 2.2.6-1 and Table 2.2.6-1.

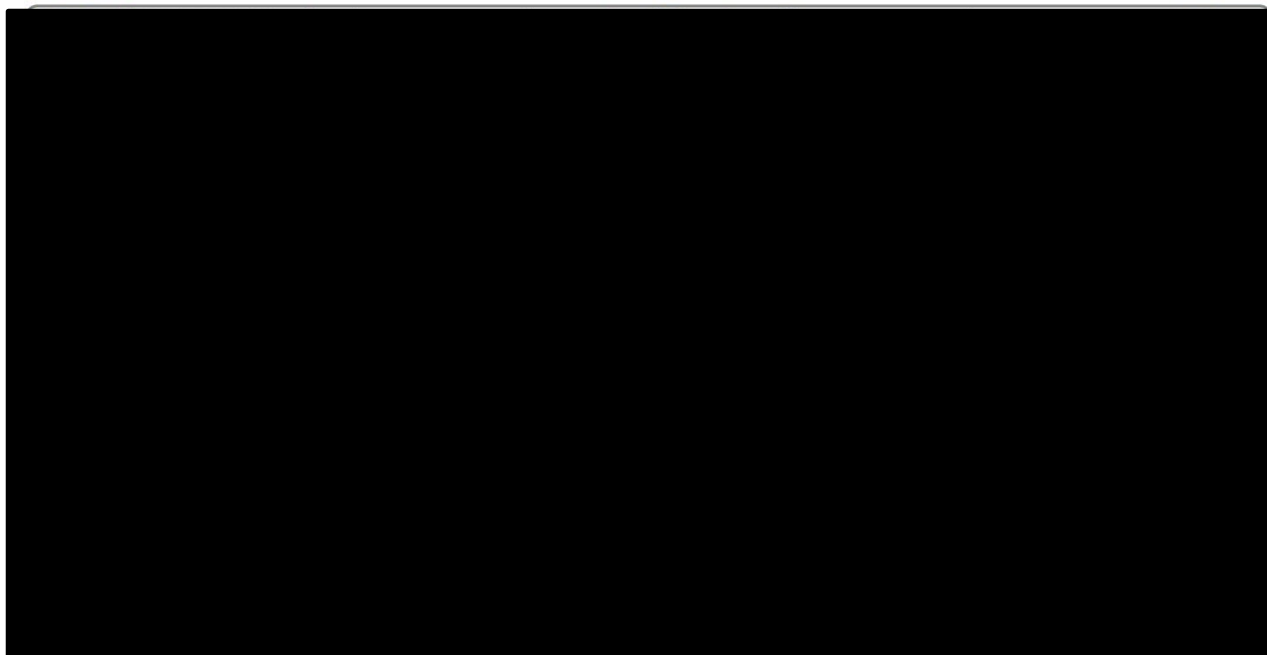


Figure 2.2.6-1. MWS Coverage.

Table 2.2.6-1. MWS Overview Description.

Architectural Components	Description
Functional Components	
Network	<ul style="list-style-type: none"> Network Network Network Network
Plans	<ul style="list-style-type: none"> Plans Plans Plans
Devices	<ul style="list-style-type: none"> Devices Devices Devices Devices Devices
Advanced mobile solutions	<ul style="list-style-type: none"> Advanced mobile solutions Advanced mobile solutions Advanced mobile solutions
Technical Components	
Coverage	<ul style="list-style-type: none"> Coverage Coverage
Speed	<ul style="list-style-type: none"> Speed Speed

Architectural Components	Description
Reliability and quality	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Interconnecting Components	
Interconnect to public networks	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Private networking	<ul style="list-style-type: none"> [REDACTED] [REDACTED]

2.2.6.1.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our approach and architecture for delivering MWS delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.2.6-2**.

Table 2.2.6-2. MWS QoS. *MWS is fully compliant, and provides the robust scalability, high reliability, and strong resilience sought by agencies.*

Architectural Components	Description
Compliance	
[REDACTED]	<ul style="list-style-type: none"> [REDACTED]
Scalability	
Spectrum and bandwidth growth	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Geographic coverage and expansion	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Reliability	
Network operations and planning	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Resilience	
AT&T disaster recovery teams and preparation	<ul style="list-style-type: none"> [REDACTED] [REDACTED]

In alignment with GSA's AUP, and to provide Government Agencies with the optimal Wireless Service experience, AT&T Wireless Services may not be used in an

unintended or abusive manner or in any way that harms the AT&T network, disrupts or degrades service, or interferes with another customer's use or enjoyment of AT&T Services.

2.2.6.1.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.6.1.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

MWS has no service-specific requirements indicated in the RFP.

2.2.6.1.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for MWS are protected from information breaches, unauthorized access and supply chain risks

2.2.6.1.2 Technical Response for WS [L.29.2.1; M.2.1]

2.2.6.1.2.1 Service Description and Functional Definition [L.29.2.1; C.2.6.1; C.2.6.1.1]

Agencies will receive a solution that provides full service, scope, and functional capabilities, as described in **Table 2.2.6-4**.

Table 2.2.6-4. MWS Service Scope and Functional Capabilities. Agencies will receive MWS that is engineered to provide quality mobile communications

Solution Element	Description
Wireless network	
Wireless plans	
Wireless equipment	
Custom solutions	
Proprietary technology	

2.2.6.1.2.2 Standards [L.29.2.1; C.2.6.1.2]

AT&T will comply with all standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.2.6.1.2.3 Connectivity [L.29.2.1; C.2.6.1.3]

AT&T will comply with all connectivity instances listed in the RFP, as applicable.

2.2.6.1.2.4 Technical Capabilities [L.29.2.1; C.2.6.1.4]

Agencies will receive MWS that [REDACTED]. All proposed technical capabilities are described in **Table 2.2.6-5**.

Table 2.2.6-5. MWS Technical Capabilities. Agencies will receive MWS with the basic technical capabilities required to offer reliable and secure mobile communications.

#	Technical Capability		Description
1.	Originate and receive calls to/ from other networks	[REDACTED]	[REDACTED]
2.	Provide mobile devices	[REDACTED]	[REDACTED]
3.	Plans and plan aspects	Meets	<ul style="list-style-type: none"> b) Data Add-On Service Plans including data (email, Internet access, video, Multimedia Messaging Service (MMS) and other data) added to voice service plans. c) Data only Service Plans including emails, Internet access, video, MMS, and other data transport not combined with voice service plans.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this document.

2.2.6.1.2.5 Features [L.29.2.1; C.2.6.2]

Table 2.2.6-6.

#	Feature	Required	Description
1.	Wireless priority services support	Yes	Wireless priority services support
2.	Directory assistance	Yes	Directory assistance
3.	Domestic to non-Domestic calling	Yes	Domestic to non-Domestic calling
4.	International mobile roaming (optional)	Yes	International mobile roaming (optional)
5.	Personal hotspot	Yes	Personal hotspot
6.	Indoor cellular systems	Yes	Indoor cellular systems
7.	Push to talk (optional)	Yes	Push to talk (optional)

AT&T Wireless Service is compatible with interfaces in RFP Section C.2.6.3.1, as applicable.

AT&T Wireless Service meets all KPIs listed in RFP Section C.2.6.4.1.

2.2.7 Service Area: Commercial Satellite Service [C.1.8.1]

Agencies will receive experienced satellite

AT&T COMSATCOM Experience

2.2.7.1.1 How AT&T Will Provide Proposed Services and Features
[L.29.2.1; M.2.1]

2.2.7.1.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

Figure 2.2.7-1 and Table 2.2.7-1.

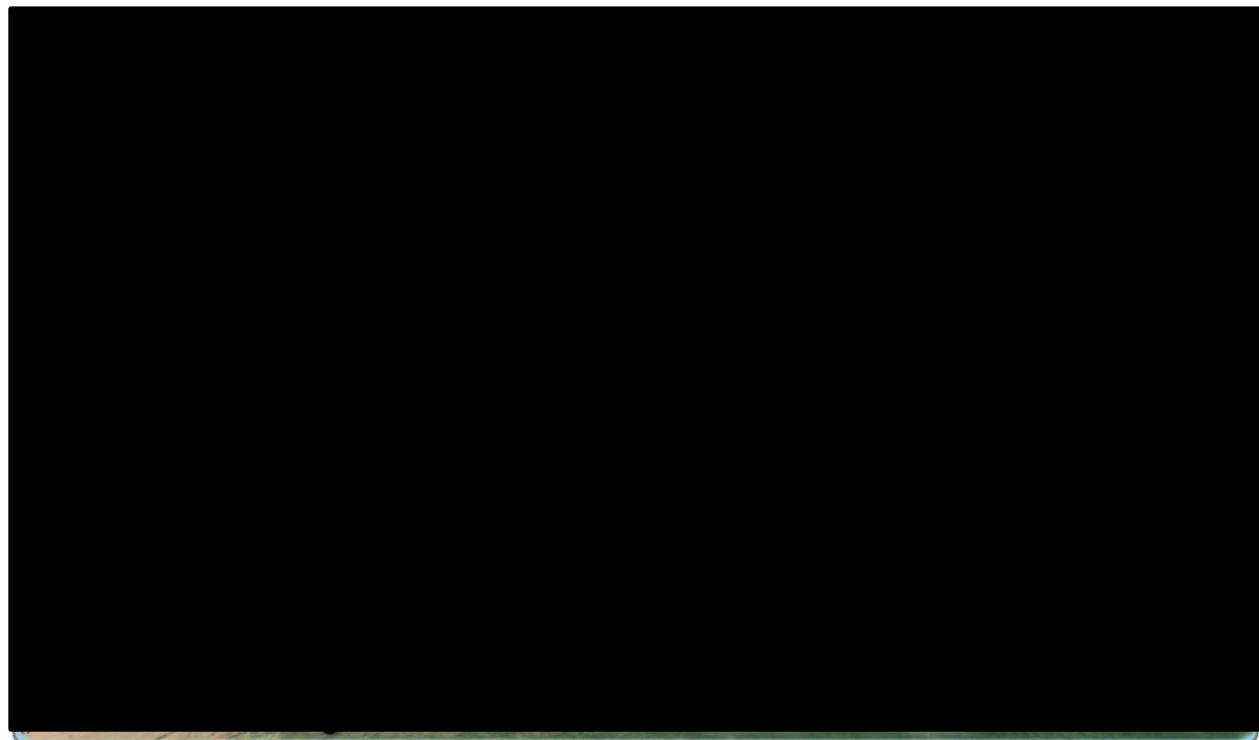
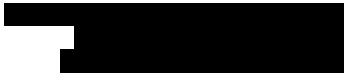


Figure 2.2.7-1. COMSATCOM Overview.

Table 2.2.7-1.

Architectural Components	Description
	
	
	
	
	
	



Architectural Components	Description
Remote earth terminals	<ul style="list-style-type: none"> Provides both leased and owned remote-side satellite earth terminal (ET) options with a range of capability sets, sizes/throughputs, air interfaces, and modulation schema May be fixed, vehicle transported, and/or man transportable, as defined in a TO Will conform to required standards, including Military Standard (MIL-STD)-188-164 with associated modems conforming to MIL-STD-188-165

2.2.7.1.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Table 2.2.7-2.

Table 2.2.7-2. COMSATCOM QoS.

Architectural Components	Description

2.2.7.1.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

Section 2.2.7.1.2.5.

2.2.7.1.2.1 Service Description and Functional Definition [L.29.2.1; C.2.7.1; C.2.7.1.1]

Table 2.2.7-4.

Table 2.2.7-4. COMSATCOM Service Scope and Functional Capabilities.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this document.

Solution Element	Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

2.2.7.1.2.2 Standards [L.29.2.1; C.2.7.1.2]

[REDACTED]

[REDACTED]

2.2.7.1.2.3 Connectivity [L.29.2.1]

[REDACTED]

2.2.7.1.2.4 Technical Capabilities [L.29.2.1; C.2.7.1.3]

[REDACTED]

[REDACTED] Table 2.2.7-5, [REDACTED]

Section 2.2.7.1.1.1.

Table 2.2.7-5. COMSATCOM Technical Capabilities. [REDACTED]

Technical Capability	[REDACTED]	Description
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

2.2.7.1.2.5 Features [L.29.2.1; C.2.7.2]

Table 2.2.7-6,

Section 2.2.7.1.1.1.

Table 2.2.7-6. COMSATCOM Features.

#	Feature		Description
1.	Capacity		
2.	Coverage		
3.	Network monitoring and reporting		
4.	EMI/RFI mitigation		
5.	Interoperability		
6.	Information assurance		

2.2.7.1.2.6 Interfaces [L.29.2.1]

2.2.7.1.2.7 Performance Metrics [L.29.2.1; C.2.7.3]

2.2.7.2 Commercial Mobile Satellite Service (CMSS) [L.29.2.1; M.2.1; C.2.7]

AT&T offers agencies access to global satellite communications systems enabling personnel to communicate at any time or place, regardless of mission location or situation.

2.2.7.2.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.7.2.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

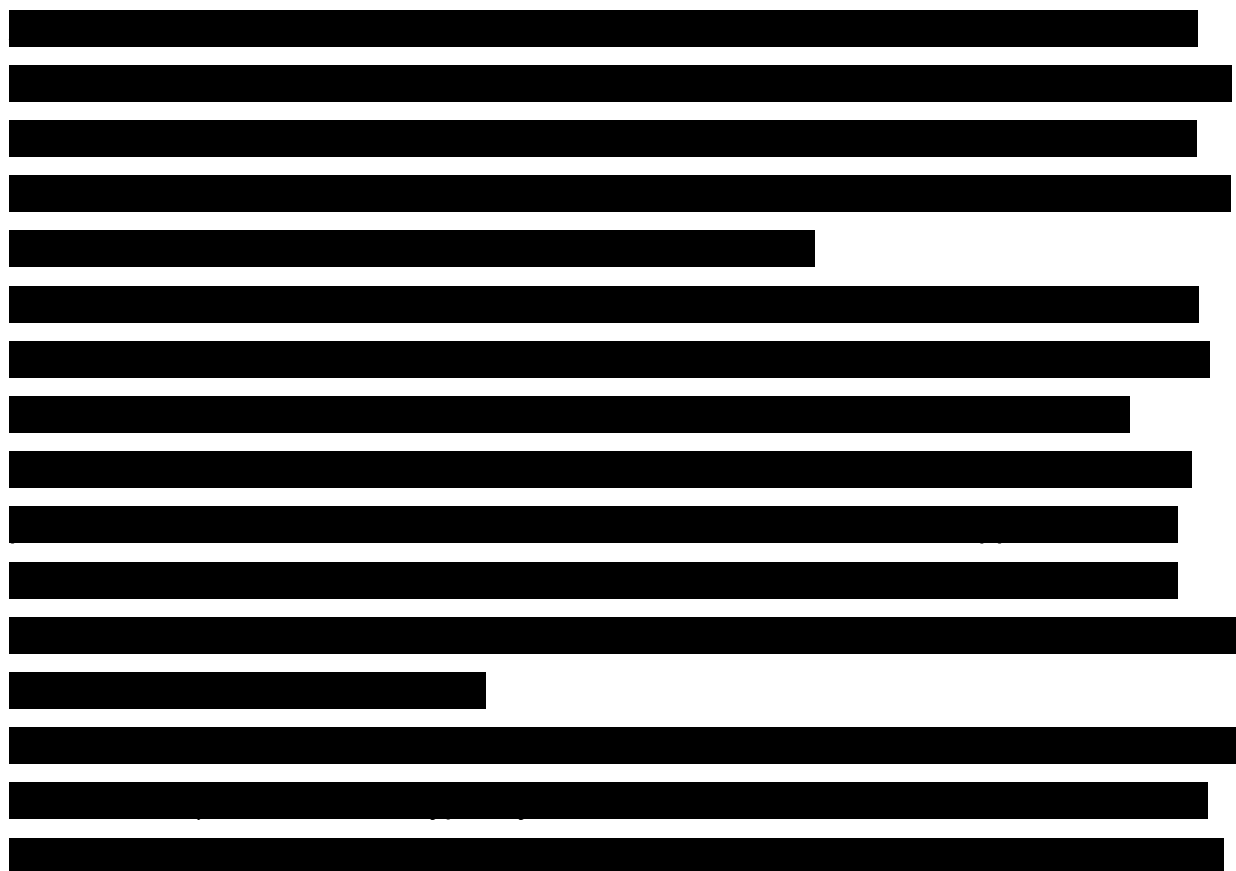


Figure 2.2.7.2-1 and Table 2.2.7.2-1.

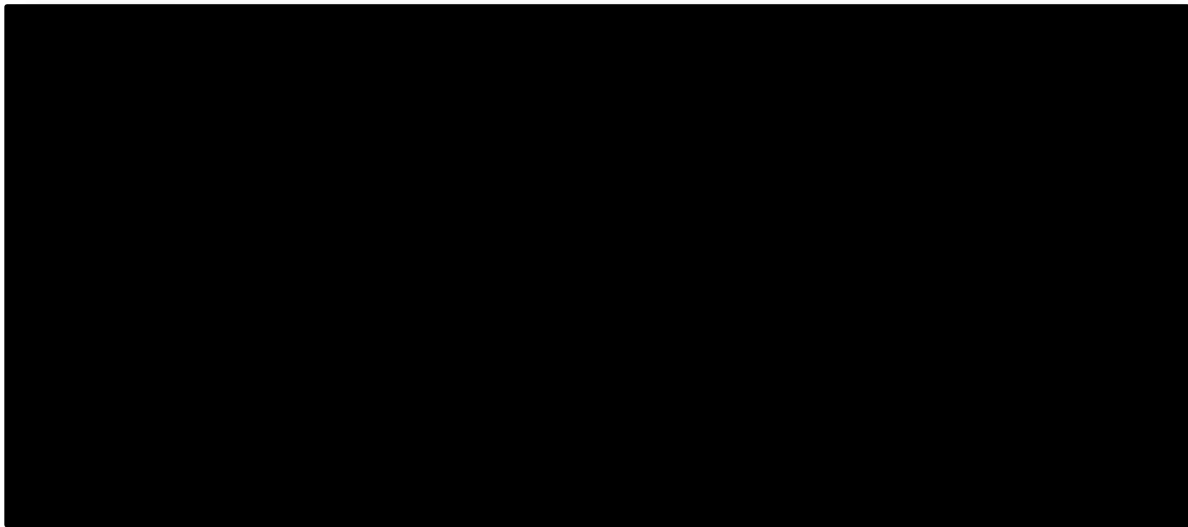


Figure 2.2.7.2-1 CMSS Overview.

Project Information		Project Details	
Project Name	Project ID	Project Manager	Project Status
Project A	101	John Doe	In Progress
Project B	102	Jane Smith	Completed
Project C	103	Mike Johnson	On Hold
Project D	104	Sarah Brown	In Progress
Project E	105	David Wilson	Completed
Project F	106	Emily Davis	On Hold
Project G	107	Chris Miller	In Progress
Project H	108	Alexander Lee	Completed
Project I	109	Olivia White	On Hold
Project J	110	Benjamin Green	In Progress

2.2.7.2.1.2 Quality of Services (QoS) [L.29.2.1(B); M.2.1(2)]

Our approach and CMSS architecture deliver compliant service as shown in **Table**

2.2.7.2-2.

Table 2.2.7.2-2. CMSS Quality of Service (QoS).

2.2.7.2.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.7.2.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

The contract indicates no CMSS-specific security requirements.

2.2.7.2.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

2.2.7.2.2 Technical Response for CMSS [L.29.2.1; M.2.1]

2.2.7.2.2.1 Service Description and Functional Definition [L.29.2.1; C.2.7.1; C.2.7.1.1]

Table 2.2.7.2-3, Section

2.2.7.2.1.1.

Table 2.2.7.2-3. CMSS Service Scope and Functional Capabilities.

Solution Element	Description
Satellite Bandwidth	
Hub Services	
Subscriber Terminals	
Proprietary Technology	

2.2.7.2.2.2 Standards [L.29.2.1; C.2.7.1.2]

2.2.7.2.2.3 Connectivity [L.29.2.1]

2.2.7.2.2.4 Technical Capabilities [L.29.2.1; C.2.7.1.3]

Table 2.2.7.2-4,

Section 2.2.7.2.1.1.

Table 2.2.7.2-4. CMSS Technical Capabilities. *Agencies will receive services that meet required technical capabilities.*

#	Technical Capability		Description
1.	Internet Access		
2.	Voice Calling		
3.	SMS Texting		
4.	Fax		

#	Technical Capability		Description
5.	Streaming Services		
6.	M2M		

2.2.7.2.2.5 Features [L.29.2.1; C.2.7.2]

2.2.7.2.2.6 Interfaces [L.29.2.1]

2.2.7.2.2.7 Performance Metrics [L.29.2.1; C.2.7.3]

2.2.8 Service Area: Managed Service [C.2.8]

2.2.8.1 Web Conferencing Service [L.29.2.1; M.2.1; C.2.8.2]

Agencies can meet their need for highly secure, feature-rich web conferencing service (WCS) through AT&T WCS. WCS enables agencies to share applications and data with remote participants in real-time. Web conferences can connect several participants or several hundred, while scheduled events and web broadcasts can reach thousands.

2.2.8.1.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.8.1.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

Agencies will benefit from our company's extensive experience providing web conferencing services.

Figure 2.2.8-1 and
Table 2.2.8-1.

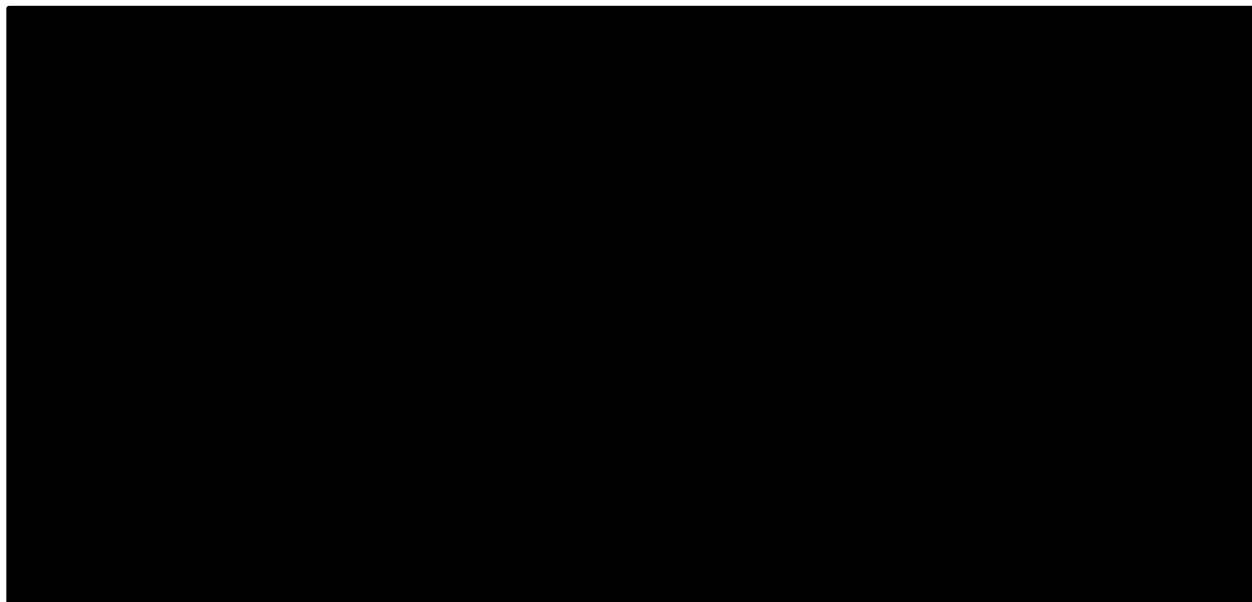


Figure 2.2.8-1. WCS Overview.

Table 2.2.8-1. WCS Overview Description. *AT&T's WCS connects authorized user devices together to deliver a common conference experience and provides each user the opportunity to interact with others in conference and participate collaboratively.*

Architectural Components	Description
Functional Components	
Web conference communication server and communication center	
Web conference client	
<ul style="list-style-type: none"> PC client Mobile client 	
Operational Components	
Event management	
Network Components	
IP transport	

2.2.8.1.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Table 2.2.8-2.

Architectural Components	Description
Compliance	
Demonstrated compliance	<ul style="list-style-type: none"> 2.2.8.1.2
Scalability	
Expanded capacity	<ul style="list-style-type: none">
Integration with audio service	<ul style="list-style-type: none">
Reliability	
Redundant distributed architecture	<ul style="list-style-type: none">
Operator support	<ul style="list-style-type: none">
High service and support availability	<ul style="list-style-type: none">
Resilience	
Resilient modular design	<ul style="list-style-type: none">
Maintenance support	<ul style="list-style-type: none">
Backup and recovery	<ul style="list-style-type: none">

2.2.8.1.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.8.1.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

WCS has no service-specific requirements indicated in the RFP.

2.2.8.1.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for WCS are protected from information breaches, unauthorized access and supply chain risks

2.2.8.1.2 Technical Response for WCS [L.29.2.1; M.2.1]

2.2.8.1.2.1 Service Description and Functional Definition [L.29.2.1; C.2.8.2.1; C.2.8.2.1.1]

Agencies receive a solution that provides full service scope and functional capabilities, as described in **Table 2.2.8-4** and described previously in **Section 2.1.8.1.1.1**.

Table 2.2.8-4. WCS Service Scope and Functional Capabilities. WCS offers a variety of convenient ways for agencies and their guests to meet, present, and interact

Solution Element	Description
Meet, present, and interact with information via a web browser	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
Share information, documents, or applications interactively	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
Connect through public internet or agency's intranet	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
Proprietary technology	<ul style="list-style-type: none"> ■ [REDACTED]

2.2.8.1.2.2 Standards [L.29.2.1; C.2.8.2.1.2]

AT&T will comply with all standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.2.8.1.2.3 Connectivity [L.29.2.1; C.2.8.2.1.3]

AT&T will comply with all connectivity instances listed in the RFP as applicable.

2.2.8.1.2.4 Technical Capabilities [L.29.2.1; C.2.8.2.1.4]

Table 2.2.8-5,

in Section 2.2.8.1.1.1.

Table 2.2.8-5

#	Technical Capability		Description
1.	Web-based collaboration		
2.	Authentication, Greeting, on-line help		
3.	Interoperates with public internet or agency intranet		
4.	Compatible user interface		
5.	Pretesting and plug-ins		

#	Technical Capability		Description
6.	Support dynamic content		
7.	Available on demand or via a scheduled reservation		
8.	Advance scheduling		
9.	Email notification with RSVP		
10.	Extend conference time and add participants		
11.	Security		
12.	Accessible via URL		
13.	Passwords		
14.	Capacity		
15.	Traversing agency firewalls		
16.	Operators		
17.	Annotation capability		
18.	Participant List		
19.	Web surfing		
20.	File transfer		
21.	Multiple presenter support		
22.	Large video webcasts		
23.	Polling and voting		
24.	Instant feedback		
26.	Print and save		
27.	Text chat		
28.	Survey capability		

2.2.8.1.2.5 Features [L.29.2.1; C.2.8.2.2]

Table 2.2.8-6, and described previously in

Section 2.2.8.1.1.1.

Table 2.2.8-6. WCS Features. Agencies receive service that meets the EIS RFP required features.

Feature	Description
RFP Required Features	
Streaming audio	
Streaming video	
Presentation replay	

2.2.8.1.2.6 Interfaces [L.29.2.1; C.2.8.2.3]

RFP identifies interfaces for WCS as “Not applicable — WCS is browser-based service”.

2.2.8.1.2.7 Performance Metrics [L.29.2.1; C.2.8.2.4; C.2.8.2.4.1]

2.2.8.2 Unified Communications Service [L.29.2.1; M.2.1; C.2.8.3]

To empower employees and increase productivity,

2.2.8.2.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.8.2.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

An increasingly diverse and mobile workforce has put workers at a disadvantage when trying to communicate using traditional technology. The Unified Communications Service (UCS) ties together the telephone, email, instant messaging, and collaboration, for desktop, mobile, and remote teleworkers. UCS merges all of these technologies into a single interoperable communications system that allows workers to stay in contact, shorten cycle times, find information, and extend the reach of their work locations. The

proposed architecture and services meet the EIS service requirements shown in **Figure 2.2.8-2** and **Table 2.2.8-7**.

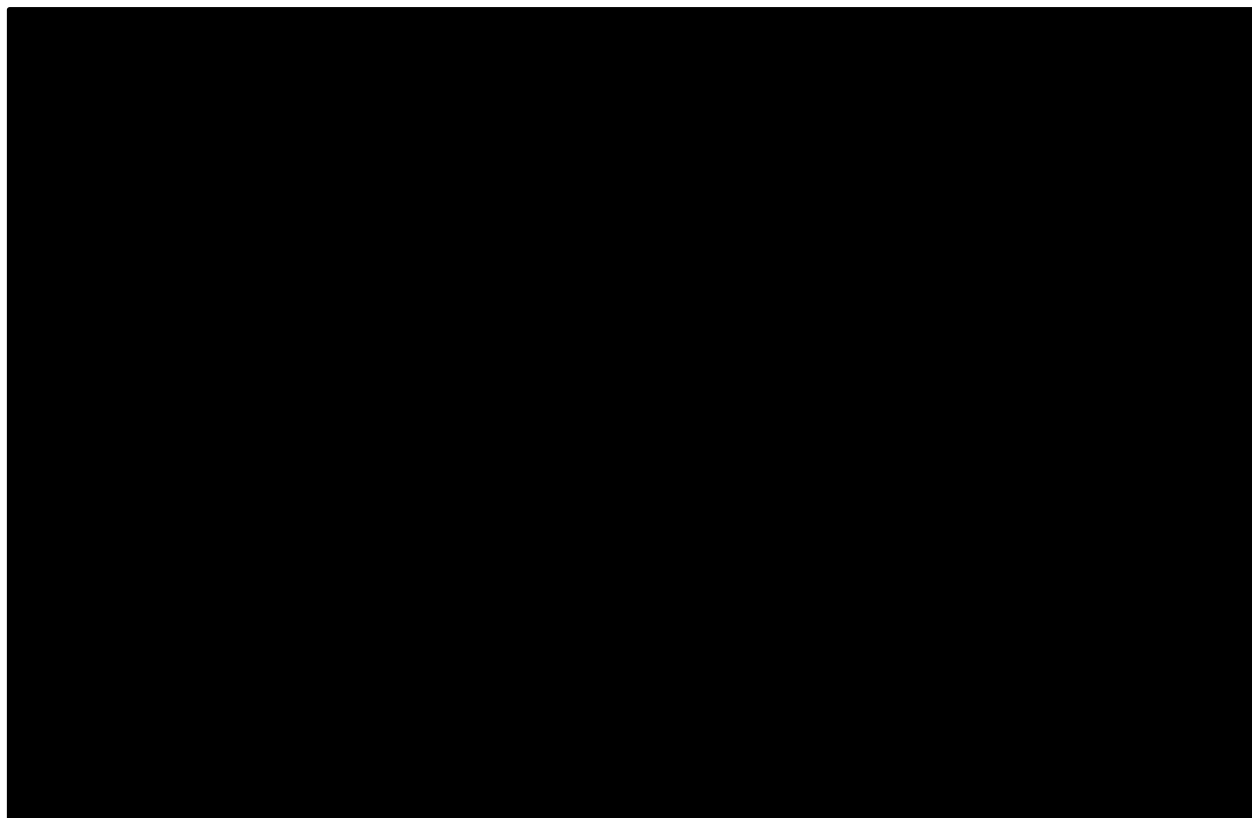


Figure 2.2.8-2. UCS Overview.

Table 2.2.8-7. UCS Overview Description. *AT&T UCS systems, networks, and components are provided in a service format called UC as a Service (UCaaS).*

Architectural Components	Description
Functional Components	
Call control	
Presence	
Calendar	
Instant messaging	

Architectural Components	Description
Message store	
Conferencing	
Contacts	
Technical Components	
FISMA UC service nodes	
IP-voice call control	
Multi-device UC client	
Operational Components	
Device management	
Service management	
Administrator's portal	
Network Components	
IP VPN	
SIP trunk	
IP phones/ soft phones	
IP to analog gateways	
VoIP capable LAN	
PC's	
Tablets (optional)	
Cellular devices	
SRST	

2.2.8.2.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our approach and architecture for delivering UCS delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.2.8-8**.

Table 2.2.8-8. UCS QoS.

Architectural Components	Description
Compliance	
Demonstrated compliance	<ul style="list-style-type: none"> Section 2.2.8.2.2
Scalability	
Modular components	<ul style="list-style-type: none">
High bandwidth capacity	<ul style="list-style-type: none">
Reliability	
Geo-redundant	<ul style="list-style-type: none">
High availability servers	<ul style="list-style-type: none">
Resilience	
Network-based service	<ul style="list-style-type: none">

2.2.8.2.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.8.2.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

UCS has no service-specific requirements indicated in the RFP.

2.2.8.2.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for UC are protected from information breaches, unauthorized access and supply chain risks

2.2.8.2.2 Technical Response for UCS [L.29.2.1; M.2.1]

2.2.8.2.2.1 Service Description and Functional Definition [L.29.2.1; C.2.8.3.1; C.2.8.3.1.1]

Agencies receive a solution that provides full service scope and functional capabilities, as described in **Table 2.2.8-10**, and described previously in **Section 2.2.8.2.1.1**.

Table 2.2.8-10. UCS Service Scope and Functional Capabilities. Agencies receive service with capability that meets service description and functional requirements.

Solution Element	Description
Hosted UC	[REDACTED]
Hybrid solutions	[REDACTED]
Premises based solutions	[REDACTED]
Proprietary technology	[REDACTED]

2.2.8.2.2.2 Standards [L.29.2.1; C.2.8.3.1.2]

AT&T will comply with all standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.2.8.2.2.3 Connectivity [L.29.2.1; C.2.8.3.1.3]

AT&T will comply with all connectivity instances listed in the RFP as applicable.

2.2.8.2.2.4 Technical Capabilities [L.29.2.1; C.2.8.3.1.4]

Agencies receive UCS [REDACTED]. All proposed technical capabilities are described in **Table 2.2.8-11**, and described previously in **Section 2.2.8.2.1.1**.

Table 2.2.8-11. UCS Technical Capabilities. Agencies receive service [REDACTED]

#	Technical Capability	Description
1.	Device support	[REDACTED]
2.	Unified messaging	[REDACTED]

Use or disclosure of data contained on this page is subject to the restriction on the title page of this document.

#	Technical Capability		Description
5.	Bandwidth management		
6.	Premises-based WAN (Optional)		
7.	Use of IP		
8.	Call quality		
9.	Security		

2.2.8.2.2.5 Features [L.29.2.1; C.2.8.3.2]

The RFP indicates no features for UCS.

2.2.8.2.2.6 Interfaces [L.29.2.1; C.2.8.3.3]

AT&T UCS is compatible with interfaces in RFP Section C.2.8.3.3, as applicable.

2.2.8.2.2.7 Performance Metrics [L.29.2.1; C.2.8.3.4; C.2.8.3.4.1]

The AT&T UCS meets all KPIs listed in RFP Section C.2.8.3.4.1.

2.2.8.3 Managed Trusted Internet Protocol Service [L.29.2.1; M.2.1; C.2.8.4]

Agencies will benefit from AT&T's MTIPS solution, which provides a robust, highly secure, and TIC 2.0-compliant means to access the Internet and other external networks.

2.2.8.3.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.8.3.1.1 Understanding [L.29.2.1(A); M.2.1(1); C.2.8.4.1]

We have extensive experience in supporting complex implementations of mission critical services for the Federal government, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Figure 2.2.8-3 and Table 2.2.8-12.

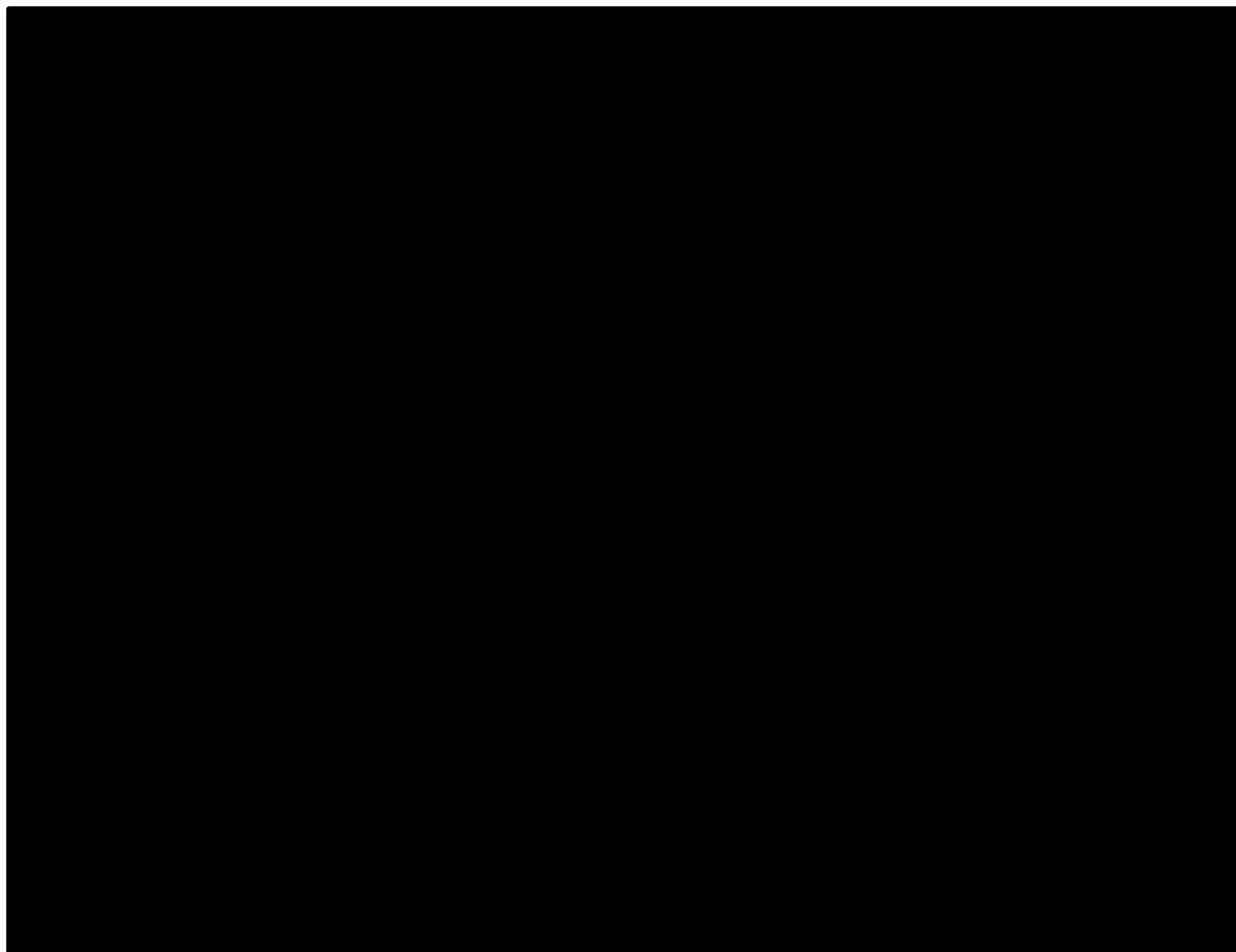


Figure 2.2.8-3. MTIPS Overview.

Table 2.2.8-12. MTIPS Overview Description. *Fuses core capabilities with innovation from AT&T Labs and the most advanced threat intelligence available, allowing MTIPS to meet today's toughest agency demands.*

Architectural Components	Description
Functional Components	
Security enforcement node	[REDACTED]
	[REDACTED]

Architectural Components	Description
	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Shared component node	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Security operations analysis center	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Security operations management center	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Technical Components	
Network-based firewall	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Email scan and filter	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Network intrusion detection/prevention systems	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Operational Components	
Threat management system	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Storage area network	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Network Components	
Border router	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Service router	<ul style="list-style-type: none"> [REDACTED] [REDACTED]
Aggregation router	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]

2.2.8.3.1.2 Quality of Services [L.29.2.1(B); M.2.1(2); C.2.8.4.1]

We have integrated [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

AT&T Consistent Compliance with DHS/GSA Requirements	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

MTIPS deliver compliant, scalable, reliable, and resilient service as shown in **Table 2.2.8-13**.

Table 2.2.8-13. MTIPS QoS.

Architectural Components	Description
Compliance	
Demonstrated compliance	[REDACTED]
Scalability	
TIC portal	[REDACTED]
Transport	[REDACTED]
Reliability	
TIC portal	[REDACTED]
Transport	[REDACTED]
Resiliency	
TIC portal infrastructure	[REDACTED]
Transport	[REDACTED]

See **Section 1.3** for AT&T service coverage for MTIPS.

2.2.8.3.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.8.3.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

See proposal **Section 2.2.8.3.2.8** for the AT&T response to these requirements.

2.2.8.3.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for MTIPS are protected from information breaches, unauthorized access and supply chain risks [REDACTED]

2.2.8.3.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3)]

Our proposed architecture

. Table 2.2.8-14 provides detailed references to our approach.

Table 2.2.8-14. Approach to External Traffic Routing Requirements. Agencies receive services

Requirement	Compliance Description
Methodology for identifying AT&T participating agency traffic for each affected service [M.2.1.4.c.i]	Section 1.4.3.1.
Anticipated technical approach, for each affected service, to redirect all participating agency internet, extranet, and interagency traffic to DHS EINSTEIN enclaves, receive processed traffic from GFP within the DHS EINSTEIN enclave, and deliver traffic to its final destination [M.2.1.4.c.ii]	Section 1.4.3.2.
Technical approach to notify DHS if any nonparticipating agency traffic will be redirected through DHS EINSTEIN enclaves [M.2.1.4.c.iii]	Section 1.4.3.3.
Control mechanisms to ensure the identification and redirection of participating agency traffic cannot be inadvertently or maliciously bypassed [M.2.1.4.c.iv]	Section 1.4.3.4.
Sensing and control mechanisms to ensure the redirection of traffic is failsafe [M.2.1.4.c.v]	Section 1.4.3.5.
Location of AT&T certified facilities [M.2.1.4.c.vi]	Section 1.4.3.6.
Availability of TS/SCI cleared personnel for Smart-Hands service of DHS-supplied equipment [M.2.1.4.c.vii]	Section 1.4.3.7.
Instrumentation to measure transport SLA KPIs [M.2.1.4.c.viii]	Section 1.4.3.8.

2.2.8.3.2 Technical Response for MTIPS [L.29.2.1; M.2.1]

2.2.8.3.2.1 Service Description and Functional Definition [L.29.2.1; C.2.8.4.1]

Agencies receive a customized MTIPS solution that provides the full service scope and functional capabilities, as described in **Table 2.2.8-15**, and described previously in **Section 2.2.8.3.1.1**.



Table 2.2.8-15 provides additional information.

Table 2.2.8-15. MTIPS Service Scope and Functional Capabilities.

Solution Element	Description
Event generators	
Event collectors	
Analysis engines	
TIC portal system logs	
Reporting	
Other Capabilities	
Proprietary technology	

2.2.8.3.2.1.1 MTIPS Context Architecture [C.2.8.4.1.1.1]

Our MTIPS framework encompasses the functional components, transport capabilities and communications paths necessary to provide subscribing agencies with highly secure Internet connections (see **Figure 2.2.8-4**).

2.2.8.3.2.1.2 TIC Portal Security Operations Center Architecture [C.2.8.4.1.1.2]

Our TIC Portal SOC systems are [REDACTED]. **Figure 2.2.8-5**

2.2.8.3.2.2 Standards [L.29.2.1; C.2.8.4.1.2]

We comply with standards listed in the RFP and with other standards referenced by the listed standards as applicable.

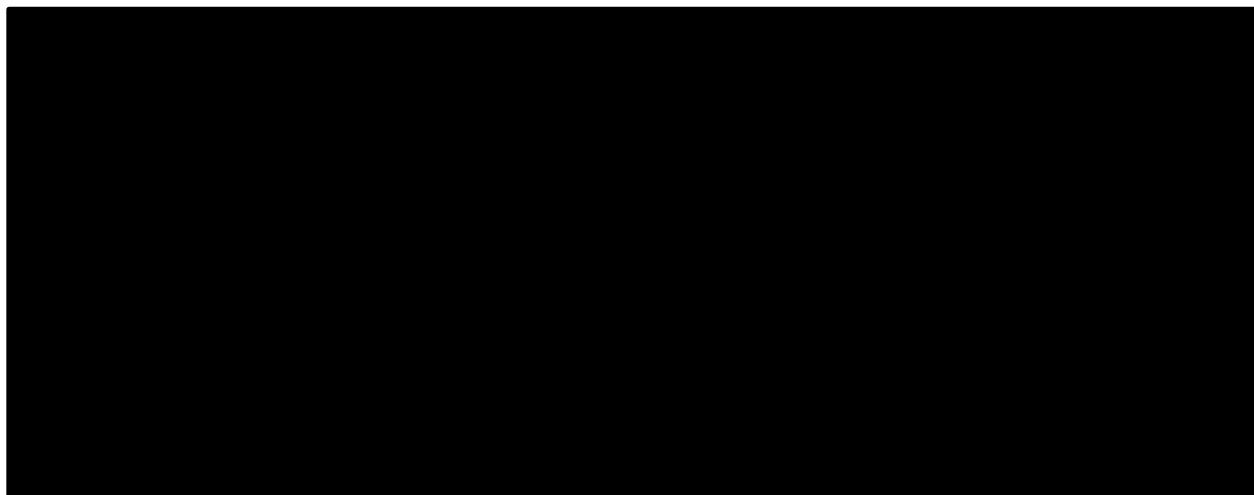


Figure 2.2.8-4. MTIPS Context Architecture. [REDACTED]

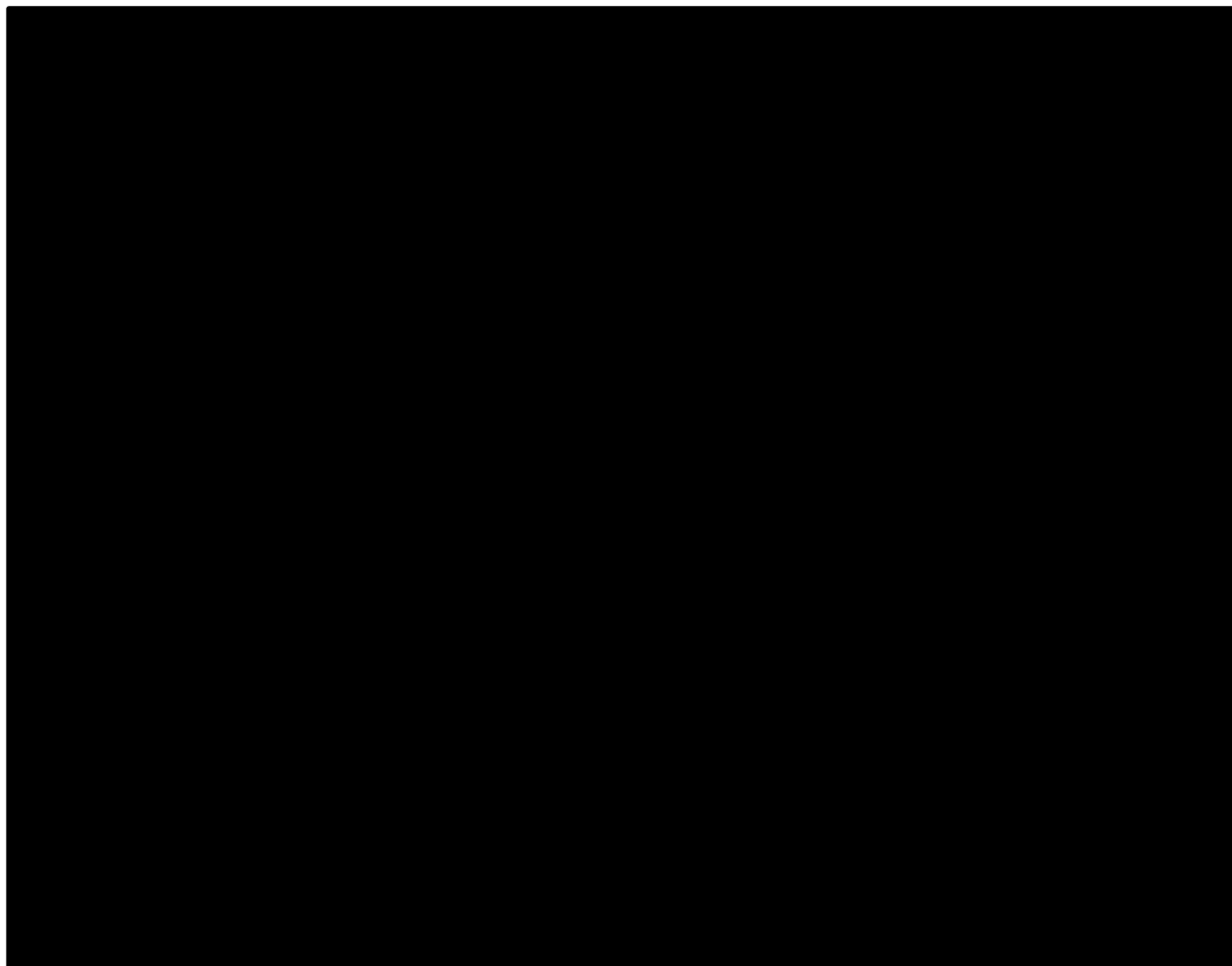


Figure 2.2.8-5. TIC Portal Security Operations Center Architecture.

2.2.8.3.2.3 Connectivity [L.29.2.1; C.2.8.4.1.3]

AT&T will comply with all connectivity instances listed in the RFP as applicable.

2.2.8.3.2.4 Technical Capabilities [L.29.2.1; C.2.8.4.1.4-C.2.8.4.1.4.2]

Agencies receive MTIPS

Table 2.2.8-16,

Section 2.2.8.3.1.1.

Table 2.2.8-16. MTIPS Technical Capabilities. Agencies receive EIS compliant MTIPS

#	Technical Capability	Description
TIC Portal Capabilities [C.2.8.4.1.4.1; C.1.8.8]		
1.	TIC portal access to external networks	

#	Technical Capability		Description
	including the internet		
2.	EINSTEIN protection		
3.	TIC portal Security Operations Center (SOC)		
4.	ICD 705 Sensitive Compartmented Information Facility (SCIF)		
5.	Content filtering/inspection of encrypted traffic		
6.	Asymmetric routing		
7.	Federal Video Relay Service (FedVRS) support		
8.	E-mail forgery protection		
9.	Signing procedures for outgoing Email		
10.	Domain Name System (DNS) and DNS Security Extensions (DNSSEC)		
11.	Uninterrupted operations		
12.	Internet Protocol Version 6 (IPv6)		
13.	Data loss/leak prevention		
MTIPS Transport Collection and Distribution Capabilities [C.2.8.4.1.4.2]			
1.	Internet-bound traffic traverses one of two TIC portals		
2.	Agency trusted domain (DMZ)		

#	Technical Capability		Description
3.	Interagency traffic classified as external connection		

2.2.8.3.2.5 Features [L.29.2.1; C.2.8.4.2]

Agencies receive established MTIPS t All
proposed features are described in **Table 2.2.8-17** and described previously in
Section 2.2.8.3.1.1.

Table 2.2.8-17. MTIPS Features. *Agencies receive service*

#	Feature		Description
1.	Encrypted traffic		
2.	Agency security policy enforcement		
3.	Forensic analysis		
4.	Custom reports		
5.	Agency SOC/NOC console		
6.	Custom security assessment and authorization support		
7.	External network connection		

#	Feature		Description
8.	Encrypted DMZ		[REDACTED]
9.	Remote access		[REDACTED]
10.	Extranet connections		[REDACTED]
11.	Inventory mapping service		[REDACTED]

2.2.8.3.2.6 Interfaces [L.29.2.1; C.2.8.4.3]

AT&T MTIPS is compatible with interfaces in RFP Section C.2.8.4.3, as applicable.

2.2.8.3.2.7 Performance Metrics [L.29.2.1; C.2.8.4.4-C.2.8.4.4.2]

AT&T's MTIPS meets all KPIs in RFP Section C.2.8.4.4.1 and C.2.8.4.4.2.

2.2.8.3.2.8 MTIPS Security Requirements [L.11; C.2.8.4.5]

All of the MTIPS security requirements indicated in RFP Section C.2.8.5.4 are addressed in proposal **Appendix B**, MTIPS Risk Management Framework Plan prepared in accordance with NIST SP 800-37. This plan includes all requirements related to the following paragraphs under RFP Section C.2.8.5.4:

- General Security Compliance Requirements [C.2.8.4.5.1]
- Security Compliance Requirements [C.2.8.4.5.2]
- Security Assessment and Authorization (A&A) [C.2.8.4.5.3]
- System Security Plan [C.2.8.4.5.4]
- Additional Security Requirements [C.2.8.4.5.5]
- Personnel Background Investigation Requirements [C.2.8.4.5.5-1]

Our MTIPS service supports a full suite of Internet access, protection and analysis services for Networkx customers. **Table 2.2.8-18** delineates additional service-specific security capabilities delivered to agencies.

Table 2.2.8-18. MTIPS Service-Specific Security Capabilities. *Agencies receive highly secure services based on our overall architecture and service-specific capabilities*

Capability	Description
Stateful firewall	
URL filtering	
Intrusion detection system	
Web proxy	
Packet capture	

2.2.8.4 Managed Security Service [L.29.2.1; M.2.1; C.2.8.5]

Agencies

and
helps maintain continuity of operations,
mission progress, and accomplishment.

2.2.8.4.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.8.4.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

AT&T understands that as agencies add new services and applications based on evolving technology in the IT arena, they seek advanced integrated security solutions from a proven and trusted provider to safeguard their infrastructure, systems and data against sophisticated and mobile cybercriminals. We have decades of experience working with government agencies and commercial enterprises on their information security planning, implementation, and management. Every day, we successfully thwart real-world threats posed to our own assets.

With one of the largest networks in the world, we apply our own expertise to protect your business. The expertise behind our security

services stems from our engineers in AT&T Labs who have made significant contributions to this field. Our security consultants stay abreast of current issues through participation in news groups and security forums, continuous education, and actual resolution of client security issues. We bring this breadth of expertise to protect your network. We have a long legacy of developing security services that answer the need to address a defense in depth architecture, from the information level to the network level. AT&T proposed architecture and services meet EIS service requirements as shown in **Figure 2.2.8-6** and **Table 2.2.8-19**.

AT&T MSS Experience and Accomplishments

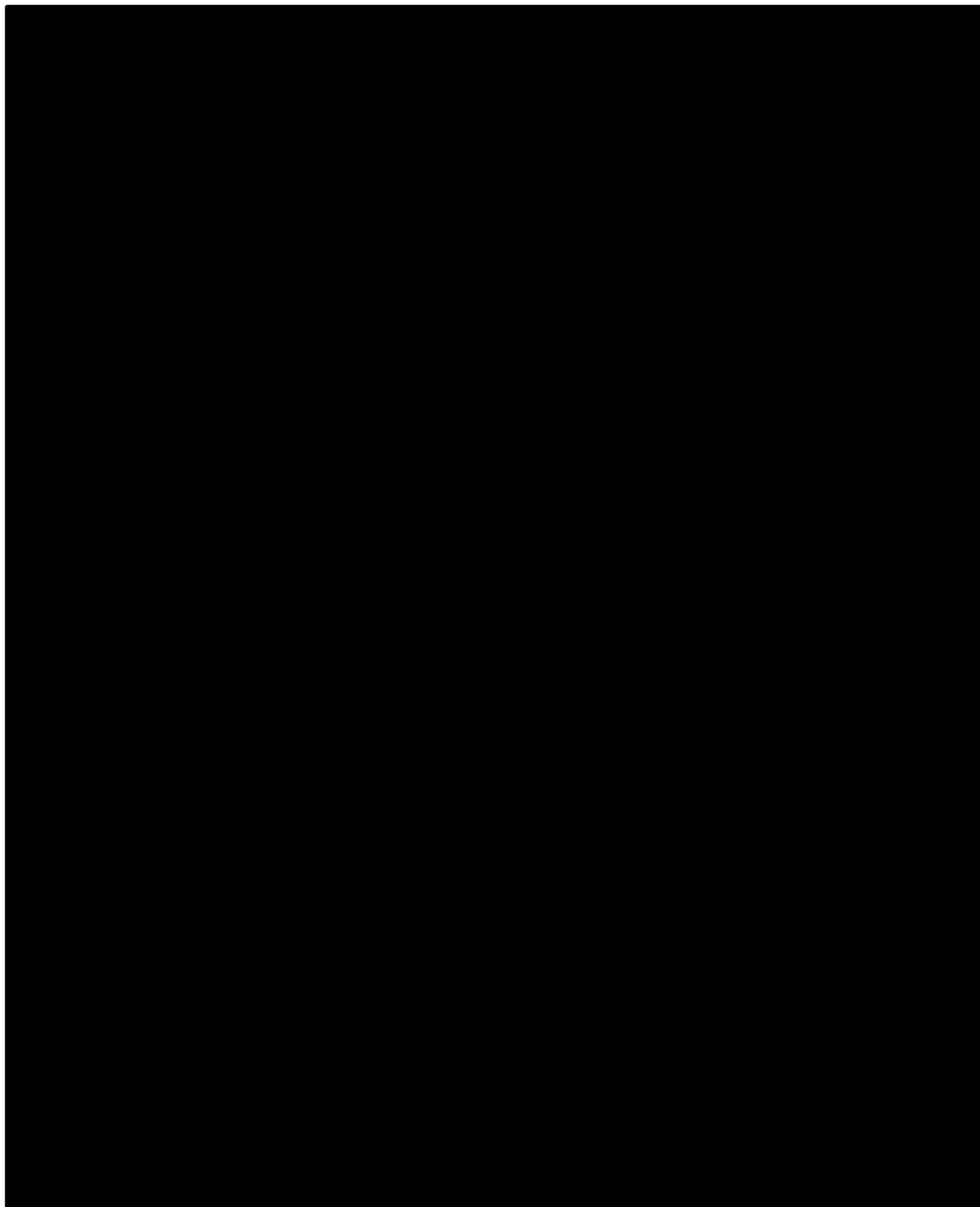


Figure 2.2.8-6. MSS Overview.

Table 2.2.8-19. MSS Overview Description. MSS components have

Architectural Components	Description
Functional Components	
Security professional services	
Technical Components	
Next-generation firewall appliances	
Premises and host intrusion/prevention	
Secure web proxy	
Web application firewall appliances	
Vulnerability scanning servers	
DDoS scrubbers	
Secure web portal	
Email cloud-based security	
Cloud-based DNS	
Operational Components	
Security/Network Operations Centers (S/NOC)	
AT&T Labs	
Aurora	
Flood	
Storm	
Daytona® database	

Architectural Components	Description
Network Components	
VPNS, ETS, and IPS	
AT&T global network	
DMZ, Extranet, and VPNs	

2.2.8.4.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our approach and architecture for delivering MSS delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.2.8-20**.

Table 2.2.8-20. MSS QoS. MSS is fully compliant, and provides robust scalability, high reliability, and strong resilience sought by GA and agencies. Service quality

Architectural Components	Description
Compliance	
Demonstrated compliance	<ul style="list-style-type: none"> Section 2.2.8.4.2
Scalability	
Support for various sized environments	<ul style="list-style-type: none"> Supports solutions that scale from small, home office environments to large globally distributed organization networks.
Reliability	
State of the art technology, services and capabilities	<ul style="list-style-type: none"> Continuously provides a healthy and highly secured operating environment in the face of evolving threats
High availability	<ul style="list-style-type: none"> Provides redundant configurations that meet agency KPI requirements.
Resilience	
Integration of services	<ul style="list-style-type: none"> Integrates multiple services and capabilities to provide agencies a resilient defense-in-depth approach to protecting their networks.
Ecosystem of suppliers	<ul style="list-style-type: none"> Allows AT&T to use the industry-leading suppliers and technologies to continue to provide the most advanced security solutions with the ever-changing security landscape.
Open standards compliance	<ul style="list-style-type: none"> Supports open standards to provide independence from particular vendors and proprietary technologies.

See **Section 1.3** for AT&T service coverage for MSS.

2.2.8.4.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.8.4.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

AT&T

Section 2.2.8.4.1.1

Section 2.2.8.4.2.

2.2.8.4.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for MSS are protected from information breaches, unauthorized access and supply chain risks [REDACTED]

2.2.8.4.2 Technical Response for MSS [L.29.2.1; M.2.1]







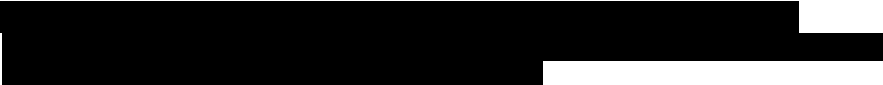
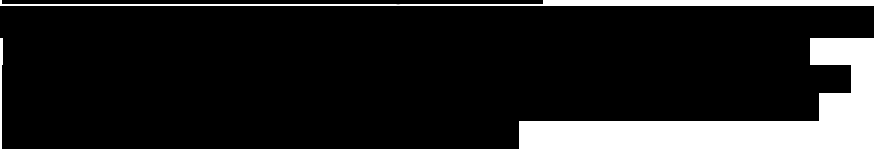



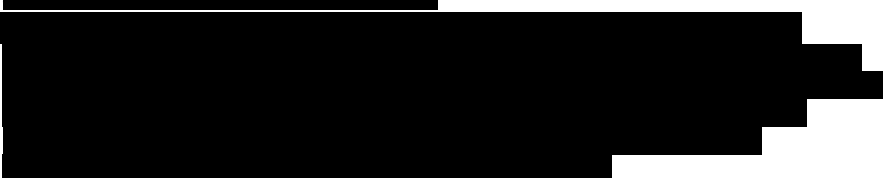
2.2.8.4.2.1 Service Description and Functional Definition [L.29.2.1; C.2.8.5.1; C.2.8.5.1.1]

Agencies receive a solution that provides the full service scope and functional capabilities, as described in **Table 2.2.8-22**, and described previously in **Section 2.2.8.4.1.1**.

Table 2.2.8-22. MSS Service Scope and Functional Capabilities.

Solution Element	Description
Managed Prevention Service (MPS)	
Monitor hosts and network traffic, and analyze network protocol and application activity to identify and mitigate suspicious activity	[REDACTED]
Managed firewalls	[REDACTED]
Host-based threat mitigation	[REDACTED]
Email-based threat mitigation	[REDACTED]
DNS-based threat mitigation	[REDACTED]
Proprietary technology	[REDACTED]

Solution Element	Description
Vulnerability Scanning Service (VSS)	
Search for security holes, flaws, and exploits on agency systems, networks and applications	<ul style="list-style-type: none"> Search for security holes, flaws, and exploits on agency systems, networks and applications Search for security holes, flaws, and exploits on agency systems, networks and applications
Continuously updated vulnerability database	<ul style="list-style-type: none"> Continuously updated vulnerability database
Simulate a real intrusion in a controlled environment	<ul style="list-style-type: none"> Simulate a real intrusion in a controlled environment
Perform external scans	<ul style="list-style-type: none"> Perform external scans Perform external scans
Perform internal scan	<ul style="list-style-type: none"> Perform internal scan Perform internal scan
Proprietary technology	<ul style="list-style-type: none"> Proprietary technology
Incident Response Service (INRS)	
Proactive activities, reactive activities, and forensics services to assist in apprehending and prosecuting offenders	<ul style="list-style-type: none"> Proactive activities, reactive activities, and forensics services to assist in apprehending and prosecuting offenders Proactive activities, reactive activities, and forensics services to assist in apprehending and prosecuting offenders Proactive activities, reactive activities, and forensics services to assist in apprehending and prosecuting offenders Proactive activities, reactive activities, and forensics services to assist in apprehending and prosecuting offenders
Proprietary technology	<ul style="list-style-type: none"> Proprietary technology Proprietary technology Proprietary technology Proprietary technology
Trusted Internet Connection Service (TICS)	

Solution Element	Description
Compliance	<ul style="list-style-type: none">   Figure 2.2.8-7. TICS  The platform allows agency IP packets to traverse through the security stack which  
Security-as-a-Service Layer	<ul style="list-style-type: none">    
Network-as-a-Service Layer	<ul style="list-style-type: none">   

We comply with standards listed in the RFP and with other standards referenced by the listed standards as applicable.

We comply with all connectivity instances listed in the RFP as applicable.

Agencies receive MSS that meets all mandatory technical capabilities. We employ a preventative approach to help identify attacks and manage intrusions proactively by:

-
- | Age Group | Good Job (%) | Not a Good Job (%) |
|-----------|--------------|--------------------|
| 18-29 | 85 | 15 |
| 30-49 | 85 | 15 |
| 50-69 | 85 | 15 |
| 70+ | 85 | 15 |
- Table 2.2.8-1

Table 2.2.8-23

and described previously in **Section 2.2.8.4.1.1**.

Table 2.2.8-23. MSS Technical Capabilities.

#	Technical Capability		Description
Managed Prevention Service (MPS) [C.2.8.5.1.4.1]			
1.	Design and implementation services		[REDACTED]
2.	Software and hardware		[REDACTED]
3.	Load balancing		[REDACTED]
4.	Installation support		[REDACTED]

#	Technical Capability		Description
			[REDACTED]
5.	Configuration information		[REDACTED]
6.	Managed service capabilities maintenance		[REDACTED]
7.	Identification and authentication controls		[REDACTED]
8.	Bug fixes and patches		[REDACTED]
9.	Patches and bug fixes		[REDACTED]
10.	Configuration and management		[REDACTED]
11.	MPS hardware/software components		[REDACTED]
12.	Service performance		[REDACTED]
13.	Security		[REDACTED]
14.	Validation activities		[REDACTED]
15.	MPS-failure		[REDACTED]
16.	Cybersecurity indicators		[REDACTED]
17.	Secure web portal		[REDACTED]
18.	DHS-provided indicators		[REDACTED]

#	Technical Capability		Description
19.	Time stamped event messages		
20.	Data separation		
21.	Secure web access		
Vulnerability Scanning Service (VSS) C.2.8.5.1.4.2]			
1.&2.	External/ internal vulnerability scanning		
1.	Network probe		
2.	Agency notifications		
3.	Secure web access		
4.	Vulnerabilities review		
5.	Scan scheduling		
6.	Nondestructive and nonintrusive vulnerability scans		
7.	Analytical alternatives		
8.	Scanning engine updates		
9.	Network scans		
Incident Response Service (INRS) [C.2.8.5.1.4.3]			
1.	Strategic planning support		

#	Technical Capability		Description
2.	Incident response support		[REDACTED]
3.	Problem detection system		[REDACTED]
4.	Analyses of suspicious security alerts		[REDACTED]
5.	Alert information		[REDACTED]
6.	Incident coordination		[REDACTED]
7.	Countermeasures		[REDACTED]
8.	Recommend fixes		[REDACTED]
9.	Provide secure web access		[REDACTED]
10.	Agency assistance and support		[REDACTED]
11.	Assist agency testing		[REDACTED]
12.	Dedicated support		[REDACTED]
13.	Post-incident services		[REDACTED]
14.	Telephone support		[REDACTED]
15.	Security professional services		[REDACTED]
16.	Security awareness training		[REDACTED]
Trusted Internet Connection Service (TICS) [C.2.8.5.1.4.4]			
1.	Adherence to current DHS CISA TIC guidance		[REDACTED]

#	Technical Capability		Description
2.	Adherence to TIC 3.0		[REDACTED]
3a.	CISA TIC Security Objectives and Security Capabilities: Enterprise-level capabilities		[REDACTED]
3b.	CISA TIC Security Objectives and Security Capabilities: Network-level capabilities		[REDACTED]
4.	Follow CISA TIC 3.0 Use Case Structure		[REDACTED]
5.	Follow CISA TIC Overlay Handbook		[REDACTED]
6.	Integrate and support CISA NCPS And CDM program requirements		[REDACTED]

2.2.8.4.2.5 Features [L.29.2.1; C.2.8.5.2]

Agencies receive established [REDACTED]

Table 2.2.8-24 [REDACTED]

Section 2.2.8.4.1.1.

Table 2.2.8-24. MSS Features. Agencies receive service [REDACTED]

#	Feature		Description
Managed Prevention Service (MPS) [C.2.8.5.1.4.1]			
a)	Firewall		[REDACTED]

#	Feature		Description
			<ul style="list-style-type: none"> • [REDACTED]
b)	Personal firewalls		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED]
c)	Network intrusion prevention system		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED] • [REDACTED] • [REDACTED]
d)	Endpoint protection		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED] • [REDACTED]
e)	Secure web proxy		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED]
f)	Inbound web filtering		<ul style="list-style-type: none"> • [REDACTED]
g)	Application-level gateway		<ul style="list-style-type: none"> • [REDACTED]
h)	Network behavior analysis		<ul style="list-style-type: none"> • [REDACTED] • [REDACTED] • [REDACTED] • [REDACTED] • [REDACTED] • [REDACTED] • [REDACTED] • [REDACTED]

#	Feature		Description
i)	Network traffic content analysis and sandboxing		
j)	Email forgery protection and filtering		
k)	Email content analysis and sandboxing		
l)	User authentication integration		
m)	DNSSEC		
n)	DNS sinkholing		
o)	Data loss prevention		
p,q)	DMZs and extranet		
r,s)	VPNs		
t)	EINSTEIN 2		
u)	Short-term storage		
v)	Long-term storage		
w)	Agency-specified policy enforcement		
Vulnerability Scanning Service (MPS) [C.2.8.5.1.4.2]			
a)	VSS API		

#	Feature		Description
Incident Reporting Service (INRS) [C.2.8.5.1.4.3]			
a)	Advanced analytics		<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]
Trusted Internet Connection Service (TICS) [C.2.8.5.1.4.4]			
a)	Encrypted Traffic		<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]
b)	Agency Security Policy Enforcement		<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
c)	Forensic Analysis		<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
d)	Custom Reports		<ul style="list-style-type: none"> ■ [REDACTED]
e)	CISA NCPS Program Protections		<ul style="list-style-type: none"> ■ [REDACTED]
f)	Custom Security A&A Support		<ul style="list-style-type: none"> ■ [REDACTED]
g (1)	External Network Connections – Route through required Policy Enforcement Points		<ul style="list-style-type: none"> ■ [REDACTED]
g (2)	External Network Connections – Encrypted, compliant to FIPS 140-2/3		<ul style="list-style-type: none"> ■ [REDACTED]

#	Feature		Description
g (3)	External Network Connections – Split Tunneling		
g (4)	External Network Connections – Performance Measures (KPI)		
h)	Support FIPS 140-2/3 encryption		
i (1)	Support Remote Access – Terminate at an appropriate point prior to routing through TICS PEPs		
i (2)	Support Remote Access – Terminate in front of the TICS PEPs		
i (3)	Support Remote Access – FIPS 140-2/3 compliant		
i (4)	Support Remote Access – No split tunneling on a VPN or remote connection		
i (5)	Support Remote Access – Use multi-factor authentication		
i (6)	Support Remote Access – Use hardened appliances		
i (7i)	Implementation – Support TLS and/or IPSec VPNs		

#	Feature		Description
i (7ii)	Implementation – Encryption compliant to FIPS 140-2/3		
i (7ii)	Implementation – Multi-factor authentication		
i (7iv)	Implementation – Separate remote access enclave		
i (7v)	Implementation – Customized remote access implementations		
j)	Extranet Connections – Support dedicated extranet connections to internal partners		

2.2.8.4.2.6 Interfaces [L.29.2.1; C.2.8.5.3]

AT&T proposed approach is compatible with interfaces in RFP Section C.2.8.5.3, and interfaces specified for VPNS in RFP Section C.2.1.1.1, for ETS in RFP Section C.2.1.2; and IPS, in RFP Section C.2.1.7.

2.2.8.4.2.7 Performance Metrics [L.29.2.1; C.2.8.5.4; C.2.8.5.4.1]

AT&T MSS meets all KPIs listed in RFP Section C.2.8.5.4.1.

2.2.8.5 Managed Mobility Service [L.29.2.1; M.2.1; C.2.8.6]

To provide agencies with a mobilized workforce, AT&T proposes a Managed Mobility Service (MMS) that enforces policies and procedures on devices (including BYOD), manages devices, data, applications, and maintains a mobile environment backed by network security. The benefit is a managed transition to a mobilized workforce that puts actionable information at the right place at the right time.

2.2.8.5.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.8.5.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

AT&T MMS provides a comprehensive range of Mobile Device Management (MDM), Mobile Application Management (MAM), and Mobile Content Management (MCM) solutions, allowing agencies to mobilize the workforce by managing the mobile work experience on devices backed with our network security while protecting sensitive data.

The offered MDM, MAM, and MCM

Figure 2.2.8-8 and Table 2.2.8-25.

Figure 2.2.8-8. MMS Overview.

Table 2.2.8-25. MMS Overview Description.

Architectural Components	Description
Functional Components	
Mobile device mgmt.	
Mobile application mgmt.	
Mobile content mgmt.	
Operational Components	

Architectural Components	Description
Administrators	
Users	
AT&T support	
Network Components	
Wireless networks	
MMS platform	
Smartphones and tablets	
Operating systems	
Mobile client	
Mobile application store	
MMS console/portal	

2.2.8.5.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our approach and architecture for delivering MMS delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.2.8-26**.

Table 2.2.8-26. MMS QoS. MMS is fully compliant, and provides robust scalability, high reliability, and strong resilience sought by agencies.

Architectural Components	Description
Compliance	
Demonstrated compliance	Section 2.2.8.5.2
Scalability	
Modular architecture	
Mass deployment tools	
Reliability	
User support	
High availability	
AT&T mobility network	
Resilience	
Help desk services	
Integrated training	

2.2.8.5.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.8.5.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

MMS security related capabilities are indicated in RFP Section C.2.8.6.1.4.4, and are addressed in proposal **Section 2.2.8.5.2.4**.

2.2.8.5.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for MMS are protected from information breaches, unauthorized access and supply chain

Table 2.2.8-27.

2.2.8.5.2 Technical Response for MMS [L.29.2.1; M.2.1]

2.2.8.5.2.1 Service Description and Functional Definition [L.29.2.1; C.2.8.6.1; C.2.8.6.1.1]

Agencies receive a solution that provides full service scope and functional capabilities, as described in **Table 2.2.8-28** and described previously in **Section 2.2.8.5.1.1**.

Table 2.2.8-28. MMS Service Scope and Functional Capabilities.

Solution Element	Description
Security (C.2.8.6.1)	
Managed handheld devices (C.2.8.6.1)	
Manage enterprise data on mobile devices	
Proprietary technology	

2.2.8.5.2.2 Standards [L.29.2.1; C.2.8.6.1.2]

AT&T will comply with all standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.2.8.5.2.3 Connectivity [L.29.2.1; C.2.8.6.1.3]

AT&T will comply with all connectivity instances listed in the RFP as applicable.

2.2.8.5.2.4 Technical Capabilities [L.29.2.1; C.2.8.6.1.4-C.2.8.6.1.4.5]

Agencies receive MDM, MAM, MCM, Mobile Security (MS), and Deployment Support (DS [REDACTED]).

All proposed technical capabilities are described in **Table 2.2.8-29**, and described previously in **Section 2.2.8.5.1.1**.

Table 2.2.8-29. MMS Technical Capabilities. Agencies receive MMS tailored to the organization's needs and sensitivities, [REDACTED].

#	Technical Capability		Description
Mobile Device Management (MDM) [C.2.8.6.1.4.1]			
1.a)	Enforce enterprise rules	[REDACTED]	[REDACTED]
1.b)	Reassign to group	[REDACTED]	[REDACTED]
1.c)	Assign profile	[REDACTED]	[REDACTED]
1.d)	View required applications from a MAS	[REDACTED]	[REDACTED]
1.e)	View and run usage/ cost reports	[REDACTED]	[REDACTED]
1.f)	View and run location reports	[REDACTED]	[REDACTED]
1.g)	Integration of SDK or API framework	[REDACTED]	[REDACTED]
1.h)	Monitor MDM system	[REDACTED]	[REDACTED]
1.i)	Integrate certificates	[REDACTED]	[REDACTED]
1.j)	Perform MDM functions within a secure VPN	[REDACTED]	[REDACTED]
2.	Device enrollment [a) – s)]	[REDACTED]	[REDACTED] b) Use a [REDACTED]

#	Technical Capability		Description
			[REDACTED]
3.	Device profiles [a) – m)]		[REDACTED]
4.	Device feature management [a) – e)]	Meets	[REDACTED]
5.	Data management [a), b)]	Meets	[REDACTED]
6.	NIST SP 800-126 SCAP) for server- side components	Meets	[REDACTED]

#	Technical Capability		Description
7.	Device inventory management and reports		
8.	System performance reports		
9.	MDM security/ compliance reports		
Mobile Application Management (MAM) [C.2.8.6.1.4.2]			
1.	Application deployment [a) – e])		
2.	Mobile Application Store (MAS) [a) i.-viii]		
3.	Application security [a) – e])		

#	Technical Capability		Description
Mobile Content Management (MCM) [C.2.8.6.1.4.3]			
1.	Secure mobile access to content		
2.	Protection of sensitive content		
3.	Central application		
Mobile Security Management (MSM) [C.2.8.6.1.4.4]			
1.	Enroll a device		
2.	Create whitelists/blacklists		
3.	Enrollment of untrusted users and anonymous devices		
4.	Attribute repository		
5.	Compliance rules actions		
6.	Block device/erase managed data [a) – f)]		
7.	Password policy enforcement [a) – f)]		
8.	Mask passwords		

#	Technical Capability		Description
9.	Admin user configuration change		
10.	User configuration change		
11.	Installation and configuration of authentication certificates [a) – c)]		
12.	Send/receive messages using PKI/S/MIME encryption		
13.	Restrict downloading or copying		
14.	View current GPS Location		
15.	Encryption of data in transit (FIPS 140-2)		
16.	Data protection		
17.	User authentication by PIN or password [a) – c)]		
18.	User compliance [a) – d)]		

#	Technical Capability		Description
19.	Alerting [a) – g)]		[REDACTED]
20.	Audit reports [a) – f)]		[REDACTED]
21.	Safeguard Personal Identifiable Information (PII)		[REDACTED]
Deployment Support (DS) [C.2.8.6.1.4.5]			
1.	Deployment		[REDACTED]
2.	Enterprise systems integration		[REDACTED]
3.	Training		[REDACTED]
4.	Help desk		[REDACTED]
Mobility-as-a-Service (MaaS) [C.2.8.6.1.4.6]			
1.	MWS Standards, Technical Capabilities and Features		[REDACTED]
2.	Solutions		[REDACTED]

#	Technical Capability		Description
3.	Implementation		
4.	Device issuance		
5.	Secure access		
6.	Sourcing management		
7.	Financial management		
8.	Program management		

2.2.8.5.2.5 Features [L.29.2.1; C.2.8.6.2]

Agencies receive established ACS that meets or exceeds all mandatory features. All proposed features are described in **Table 2.2.8-29a**, and described previously in **Section 2.2.5.6.1.1**.

Table 2.2.8-29a. MMS Features. Agencies can use the provided MMS features to enhance the participation, productivity, understanding, and documentation of their conference meetings.

#	Feature		Description
RFP Required Features			
1.	(Optional) Mobile Threat Protection (MTP)		
2.	(Optional) Mobile Application Vetting		
3.	(Optional) Mobile Identity Management		
4.	(Optional) Mobile Backend-as-a-Service (MBaaS)		

#	Feature		Description
5.	(Optional) Internet of Things (IoT)		<ul style="list-style-type: none"> [REDACTED] [REDACTED]

2.2.8.5.2.6 Interfaces [L.29.2.1; C.2.8.6.3]

AT&T MMS is compatible with interfaces in RFP Section C.2.8.6.3, as applicable.

2.2.8.5.2.7 Performance Metrics [L.29.2.1; C.2.8.6.4; C.2.8.6.4.1]

AT&T MMS meets all KPIs listed in RFP Section C.2.8.6.4.1.

2.2.8.6 Audio Conferencing Service [L.29.2.1; M.2.1; C.2.8.7]

Agencies will receive a highly scalable and feature-rich audio conferencing service through the AT&T ACS. ACS enables agencies to connect geographically dispersed participants in real-time using multiple reservation formats, and through a variety of dialing plans globally.

2.2.8.6.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.8.6.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

Audio conference service will provide agencies a robust, highly secure, and versatile service capable of providing telephone conferences to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Figure 2.2.8-8 and Table 2.2.8-30.

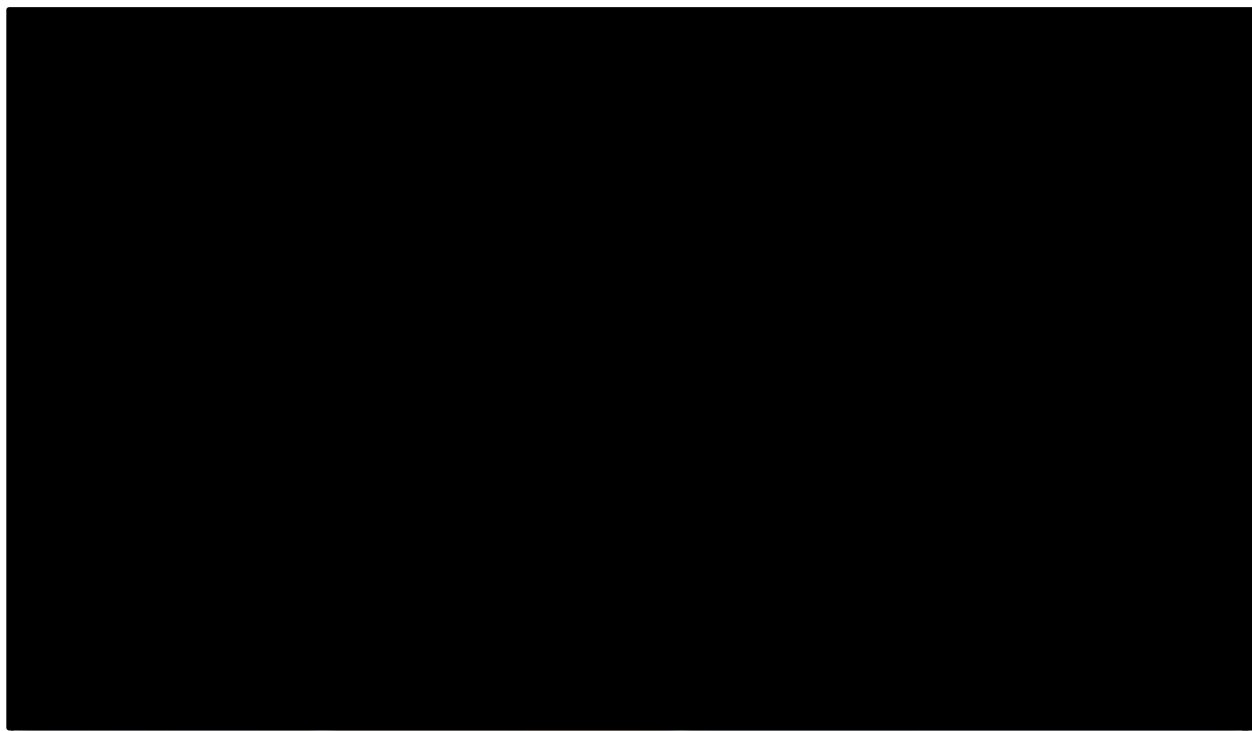


Figure 2.2.8-9. ACS Overview.

Table 2.2.8-30. ACS Overview Description. The AT&T ACS is composed of architectural components delivering an intuitive, highly secure, and feature-rich teleconference experience for hosts and participants.

Architectural Components	Description
Functional Components	
Meet-Me conference (reserved)	
Meet-Me conference (reservationless)	
Conference call email reservations	
Preset conference	
Attendant-assisted conferences	
Automatic call extension	
Automatic port expansion	
Physical/Virtual Components	

[illegible]

2.2.8.6.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our approach and architecture for delivering ACS delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.2.8-31**.

Table 2.2.8-31. ACS QoS. ACS uses architectural components that provide the required service, resulting in an offer that is fully compliant, and provides the robust scalability, high reliability, and strong resilience sought by agencies.

Architectural Components	Description
Compliance	
Demonstrated compliance	<ul style="list-style-type: none"> <div> <div></div> <div></div> </div>

Architectural Components	Description
Scalability	
Support for large conferences	
Expanded participant support	
Reliability	
Redundant distributed architecture	
Operator support	
High-quality service and customer support	
Resilience	
Modular design	
Maintenance support	
Backup and recovery	

See **Section 1.3** for AT&T service coverage for

2.2.8.6.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.8.6.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

ACS has no service-specific requirements indicated in the RFP.

2.2.8.6.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

GSA's agency customers for MMS are protected from information breaches, unauthorized access and supply chain

2.2.8.6.2 Technical Response for ACS [L.29.2.1; M.2.1]

2.2.8.6.2.1 Service Description and Functional Definition [L.29.2.1; C.2.8.7.1; C.2.8.7.1.1]

Agencies receive a solution that provides full service scope and functional capabilities specified in the SOW, as described in **Table 2.2.8-33** and described previously in

Section 2.2.8.6.1.1.

Table 2.2.8-33. ACS Service Scope and Functional Capabilities. Agencies receive a teleconferencing service that delivers an essential organizational tool for connecting geographically diverse groups for collaboration and communication sessions, with capability to meet service description and functional requirements.

Solution Element	Description
Audio conferencing service	<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
Proprietary technology	<ul style="list-style-type: none"> ■ [REDACTED]

2.2.8.6.2.2 Standards [L.29.2.1; C.2.8.7.1.2]

AT&T will comply with all standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.2.8.6.2.3 Connectivity [L.29.2.1; C.2.8.7.1.3]

AT&T will comply with all connectivity instances listed in the RFP as applicable.

2.2.8.6.2.4 Technical Capabilities [L.29.2.1; C.2.8.7.1.4]

Agencies receive ACS [REDACTED]

Table 2.2.8-34, [REDACTED]

Section 2.2.8.6.1.1.

Table 2.2.8-34. ACS Technical Capabilities. Agencies receive service [REDACTED]

#	Technical Capability	Description
1.	Multipoint bridging capability	<ul style="list-style-type: none"> ■ Simultaneously supports two-way and one-way (broadcast) conversations via a multipoint audio conference bridge ■ Allows hosts, or a subset of participants, to speak as others attend in listen-only mode ■ Allows hosts to dial-out and add new participants ■ Enables entry/exit tones that hosts can toggle on and off ■ Allows participants to join a conference in progress
2.	[REDACTED]	<ul style="list-style-type: none"> ■ [REDACTED]

#	Technical Capability		Description
	Conference setup capability		[REDACTED]
3.	Reservation system		[REDACTED]
4.	Automatic port expansion		[REDACTED]
5.	Conferee tones		[REDACTED]
6.	Participant count		[REDACTED]
7.	Roll call		[REDACTED]
8.	Attendant assistance		[REDACTED]

2.2.8.6.2.5 Features [L.29.2.1; C.2.8.7.2]

Agencies receive established ACS [REDACTED]
[REDACTED] Table 2.2.8-35, [REDACTED]

Section 2.2.8.6.1.1.

Table 2.2.8-35. ACS Features. Agencies can use the provided ACS features to enhance the participation, productivity, understanding, and documentation of their conference meetings.

#	Feature		Description
RFP Required Features			
1.	Audio recording of call		[REDACTED]
2.	Spanish language translation		[REDACTED]
3.	(Optional) Language translation		[REDACTED]
4.	Moderator-led Q&A		[REDACTED]
5.	Participant list report		[REDACTED]

#	Feature		Description
			<ul style="list-style-type: none"> ■ [REDACTED]
6.	Password-protected session		<ul style="list-style-type: none"> ■ [REDACTED]
7.	Download and replay a pre-recorded audio conference		<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]
8.	Transcription		<ul style="list-style-type: none"> ■ [REDACTED]
9.	Temporary blocking		<ul style="list-style-type: none"> ■ [REDACTED]
10.	Secure Audio Conference		<ul style="list-style-type: none"> ■ [REDACTED]
11.	Operator dial-Out		<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]
12.	Host dial-out		<ul style="list-style-type: none"> ■ [REDACTED] ■ [REDACTED]
13.	Executive conference		<ul style="list-style-type: none"> ■ [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
14.	International global meet		<ul style="list-style-type: none"> ■ [REDACTED] [REDACTED] [REDACTED] [REDACTED]
15.	Host controls		<ul style="list-style-type: none"> ■ [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

2.2.8.6.2.6 Interfaces [L.29.2.1; C.2.8.7.3]

The AT&T ACS is compatible with interfaces in RFP Section C.2.8.7.3, as applicable.

2.2.8.6.2.7 Performance Metrics [L.29.2.1; C.2.8.7.4]

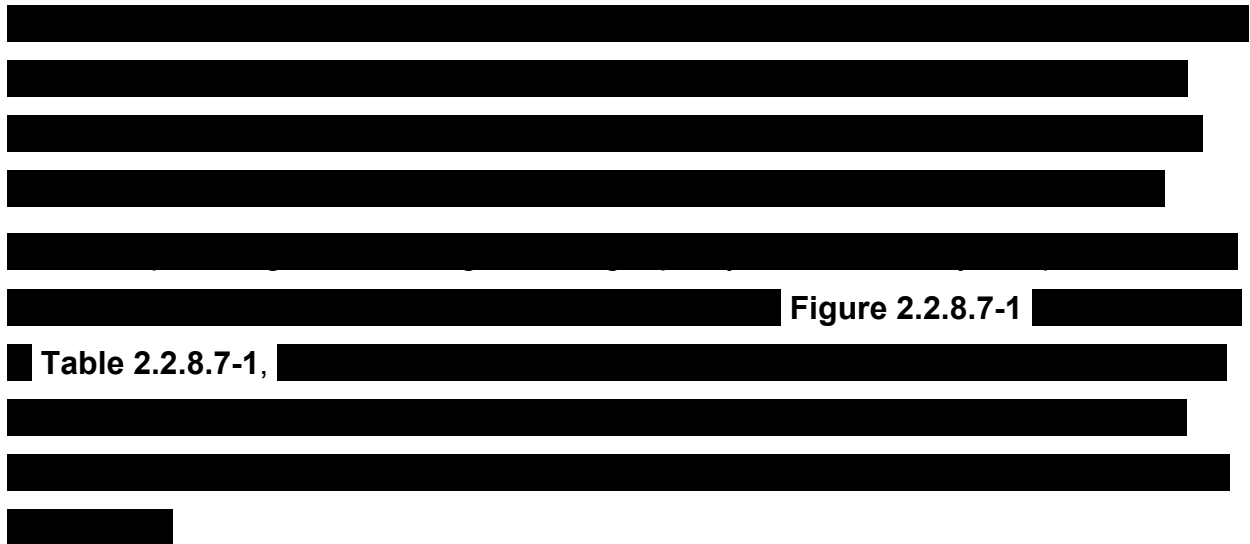
The AT&Ts ETS meets all KPIs in RFP Section C.2.8.7.4.

2.2.8.7 Video Teleconferencing Service [L.29.2.1; M.2.1; C.2.8.8]

To enable employees to better collaborate, AT&T proposes a Video Teleconference Service (VTS) that connects video teleconference rooms and desktop computers in a video and multimedia conference.

2.2.8.7.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.8.7.1.1 Understanding [L.29.2.1(A); M.2.1(1)]



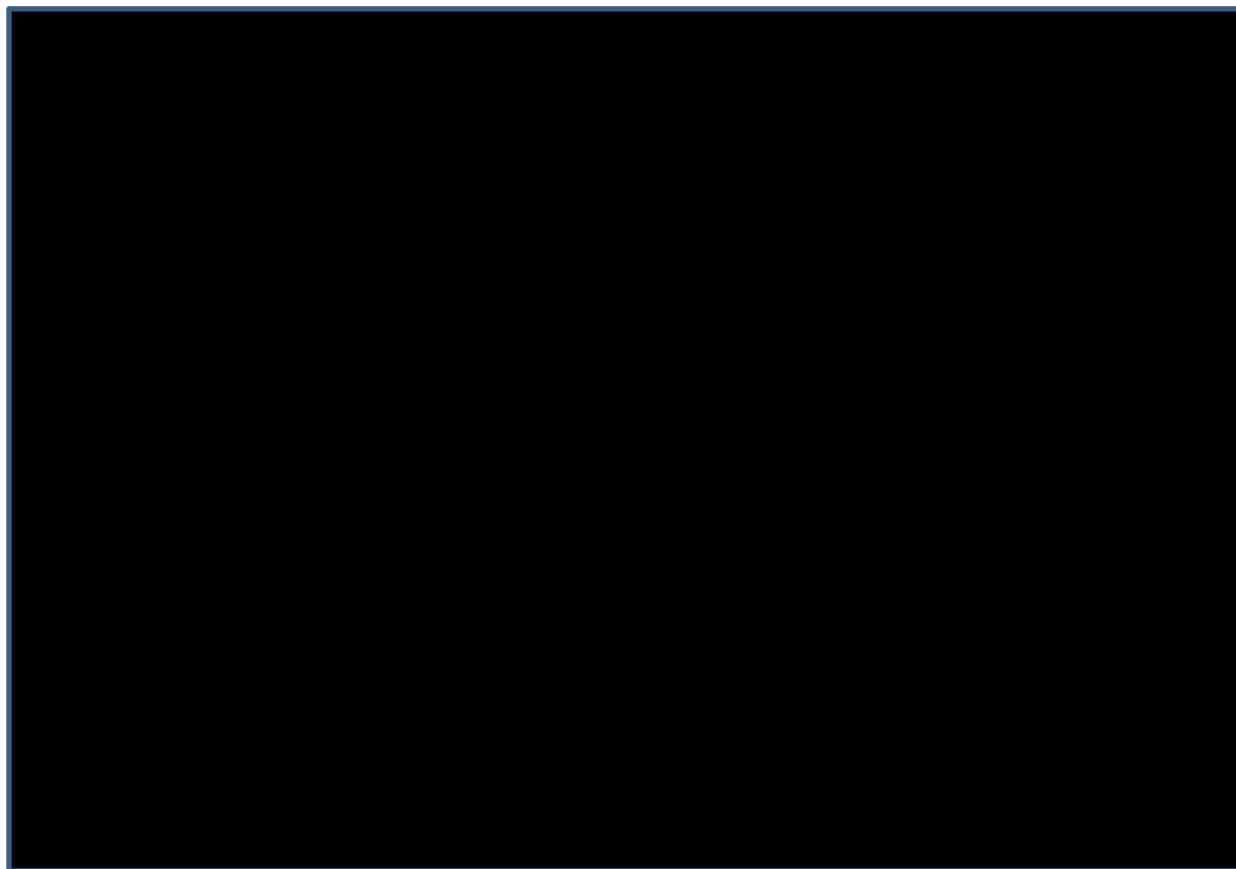


Figure 2.2.8.7-1. VTS Overview

Table 2.2.8.7-1. VTS Overview Description.

Architectural Components	Description
Functional Components	
Call control	<ul style="list-style-type: none"> [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted] [Redacted]
Viewing Options	<ul style="list-style-type: none"> [Redacted] [Redacted]



Architectural Components	Description
	[REDACTED]
Reservation System	[REDACTED]
Connectivity	[REDACTED]
Interoperability, Coding Conversion, and Rate Adaptation	[REDACTED]
Attended Service	[REDACTED]
Security	[REDACTED]
Technical Components	
VTS bridge service nodes	[REDACTED]
Web Based Reservation System	[REDACTED]
Operational Components	
Assisted Conferences	[REDACTED]
Service management	[REDACTED]
Network Components	
IP VPN	[REDACTED]
Public Internet	[REDACTED]

Architectural Components	Description
PSTN Network	[REDACTED]
Video Terminals	[REDACTED]
Desktop PC	[REDACTED]

2.2.8.7.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our approach and architecture for delivering VTSS delivers compliant, scalable, reliable, and resilient service as delineated in **Table 2.2.8.7-2**.

Table 2.2.8.7-2. VTS QoS. VTS is fully compliant, and provides robust scalability, high reliability, and strong resilience sought by agencies

Architectural Components	Description
Compliance	
Demonstrated compliance	[REDACTED]
Scalability	
Modular components	[REDACTED]
High bandwidth capacity	[REDACTED]
Reliability	
Geo-redundant	[REDACTED]
High availability servers	[REDACTED]
Resilience	
Network-based service	[REDACTED]

2.2.8.7.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.8.7.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

VTS has no service-specific requirements indicated in the RFP.

2.2.8.7.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.2.8.7.2 Technical Response for VTS [L.29.2.1; M.2.1]

2.2.8.7.2.1 Service Description and Functional Definition [L.29.2.1; C.2.8.8.1; C.2.8.8.1.1]

Table 2.2.8.7-3 Section 2.2.8.7.1.1.

Table 2.2.8.7-3. VTS Service Scope and Functional Capabilities.

Solution Element	Description
Simulated Face-to-Face Meetings	<ul style="list-style-type: none">
Point-to-point; Multipoint Conferencing	<ul style="list-style-type: none">

2.2.8.7.2.2 Standards [L.29.2.1; C.2.8.8.1.2; C.1.8.4]

2.2.8.7.2.3 Connectivity [L.29.2.1; C.2.8.8.1.3]

2.2.8.7.2.4 Technical Capabilities [L.29.2.1; C.2.8.8.1.4]

Table 2.2.8.7-4

Section 2.2.8.7.1.1.

Table 2.2.8.7-4. VTS Technical Capabilities.

#	Technical Capability		Description
1.	Video Teleconferencing		
2.	Two-way video, One-way video		
3.	Document sharing		
4.	Audio conference add-on		

#	Technical Capability		Description
5.	Bridging		
6.	Dial Modes		
7.	Operator assistance		
8.	Synchronization		
9.	Reservation-less service		
10.	Multi-point arrangements		
11.	Reservation system		
12.	Format conversion		
13.	Firewall Support		
14.	Reports		

2.2.8.7.2.5 Features [L.29.2.1; C.2.8.8.2]

Table 2.2.8.7-5.

Table 2.2.8.7-5. VTS Features.

#	Feature		Description
RFP Required Features			
1.	Attended Service		
2.	Verification		
3.	Coding Conversion		

#	Feature		Description
4.	Rate Adaption (optional)		
5.	Security- CIU (optional)		
6.	Security – Classified (optional)		

2.2.8.7.2.6 Interfaces [L.29.2.1; C.2.8.8.3; C.2.8.8.3.1]

2.2.8.7.2.7 Performance Metrics [L.29.2.1; C.2.8.8.4; C.2.8.8.4.1]

2.2.8.8 DHS Intrusion Prevention Security Service (DHS Only) [L.29.2.1; M.2.1; C.2.8.9]

Agencies will receive a fully compliant IPSS solution that is in production today delivering industry-leading performance and fully integrated with MTIPS for end-to-end agency security.

2.2.8.8.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.8.8.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

The AT&T

Agencies will benefit from IPSS by leveraging the government's knowledge and investment in identifying cyber threats while receiving an integrated commercial based service.

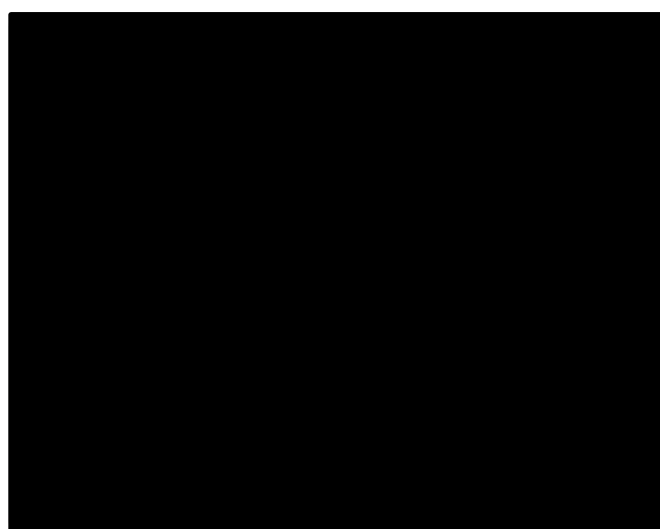


Figure 2.2.8-9. DHS IPSS Email Overview.

Our proposed architecture is shown in **Figure 2.2.8-9**, **Figure 2.2.8-10** and **Table 2.2.8-36**. Our IPSS architecture uses

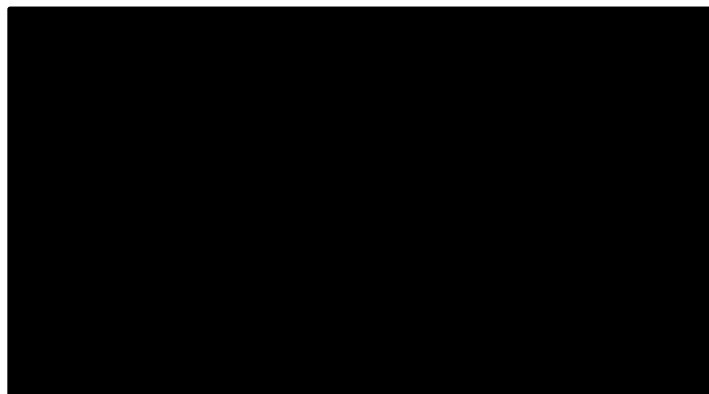


Figure 2.2.8-10. DHS IPSS DNS Overview. GSA and agencies will receive DNS security solution that blocks access to suspicious domains using government threat indicators.

Table 2.2.8-36. DHS IPSS Overview Description.

Architectural Components	Description
Physical/Logical Components	
IPSEC VPN components	
Service delivery point	
Secure enclave	
Security enforcement node	
VPN	
Premises devices	
Sink hole server	
Operational Components	
Network Management Interface (NMI)	

Architectural Components	Description
Service operations	[REDACTED]
Security operations	[REDACTED]
ISSO	[REDACTED]
Network Components	
Public Internet and boarder router	[REDACTED]
VPN and aggregation router	[REDACTED]
Extranet VPN router	[REDACTED]

The DNS solution offers protection from known malicious hosts by modifying DNS resolution responses associated with the known malicious host and replacing it with the IP address of otherwise benign servers (known as sinkhole servers or safe servers).

The caching server receives DNS transactions from the participating agency. The caching server attempts to resolve the domain name via recursive query of authoritative DNS servers on the Internet. After the server resolves the domain name, it forwards the DNS response from the DNS caching server to a separate platform that screens the domain name against a set of government-supplied indicators. If an indicator match is found, the service replaces the resolved IP address within the DNS response with the address of a sinkhole server. It also sends alert messages to the agency and DHS.

2.2.8.8.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Our approach and architecture for delivering IPSS delivers compliant, scalable, reliable, and resilient service as shown in **Table 2.2.8-37**.

Architectural Components	Description
Compliance	
Demonstrated compliance	<ul style="list-style-type: none"> <p>Section 2.2.8.8.2</p>
Scalability	
Email & DNS protection	<ul style="list-style-type: none">
MTIPS security	<ul style="list-style-type: none">
MTIPS transport	<ul style="list-style-type: none">
Reliability	
Email & DNS protection	<ul style="list-style-type: none">
MTIPS security	<ul style="list-style-type: none">
MTIPS transport	<ul style="list-style-type: none">
Resilience	
Email & DNS protection	<ul style="list-style-type: none">
MTIPS security	<ul style="list-style-type: none">
MTIPS transport	<ul style="list-style-type: none">

See **Section 1.3** for AT&T [REDACTED].

2.2.8.8.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.8.8.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

IPSS security-related requirements are indicated in the RFP service description, functional definition, technical capabilities, and features. Our proposal

Section 2.2.8.8.1.1 provides a summary of capabilities and indicates specific capabilities in proposal **Section 2.2.8.4.2. Table 2.2.8-38** delineates additional service-specific security capabilities delivered to agencies. Our IPSS [REDACTED]

Table 2.2.8-38. DNS and Email Threat Detection and Protection. *Agencies receive services*

Capability	Description
DNS threat detection and protection	
Email threat detection and protection	

2.2.8.8.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

AT&T delivers DHS IPSS Section 1.4 for AT&T security approach for this network architecture.

2.2.8.8.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3)]

Our proposed architecture

Table 2.2.8-39

Table 2.2.8-39. Approach to External Traffic Routing Requirements. *Agencies receive*

Requirement	Compliance Description
Methodology for identifying AT&T participating agency traffic for each affected service [M.2.1.4.c.i]	Section 1.4.3.1.
Anticipated technical approach, for each affected service, to redirect all participating agency Internet, extranet, and interagency traffic to DHS EINSTEIN enclaves, receive processed traffic from GFP within the DHS EINSTEIN enclave, and deliver traffic to its final destination [M.2.1.4.c.ii]	Section 1.4.3.2.
Technical approach to notify DHS if any nonparticipating agency traffic will be redirected through DHS EINSTEIN enclaves [M.2.1.4.c.iii]	Section 1.4.3.3.
Control mechanisms to ensure the identification and redirection of participating agency traffic cannot be inadvertently or maliciously bypassed [M.2.1.4.c.iv]	Section 1.4.3.4.
Sensing and control mechanisms to ensure the redirection of traffic is failsafe [M.2.1.4.c.v]	Section 1.4.3.5.
Location of AT&T certified facilities [M.2.1.4.c.vi]	Section 1.4.3.6.

Requirement	Compliance Description
Availability of TS/SCI cleared personnel for Smart-Hands service of DHS-supplied equipment [M.2.1.4.c.vii]	Section 1.4.3.7.
Instrumentation to measure transport SLA KPIs [M.2.1.4.c.viii]	Section 1.4.3.8.

2.2.8.8.2 Technical Response for DHS-IPSS [L.29.2.1; M.2.1]

2.2.8.8.2.1 Service Description and Functional Definition [L.29.2.1; C.2.8.9.1; C.2.8.9.1.1]

Agencies will receive an IPSS solution that provides indicator management, detection, response and protection, and alerting and reporting for both email and DNS, as described in **Table 2.2.8-40** and described previously in **Section 2.2.8.8.1.1**.

Table 2.2.8-40. IPSS Service Scope and Functional Capabilities. *Agencies receive service*

Solution Element	Description
Indicator management	<ul style="list-style-type: none"> Indicator management Indicator management Indicator management Indicator management
DNS threat detection and countermeasures	<ul style="list-style-type: none"> DNS threat detection and countermeasures DNS threat detection and countermeasures DNS threat detection and countermeasures DNS threat detection and countermeasures
Email threat detection and countermeasures	<ul style="list-style-type: none"> Email threat detection and countermeasures Email threat detection and countermeasures Email threat detection and countermeasures Email threat detection and countermeasures
Response and protect	<ul style="list-style-type: none"> Response and protect Response and protect Response and protect Response and protect
Alert and reporting	<ul style="list-style-type: none"> Alert and reporting Alert and reporting Alert and reporting

2.2.8.8.2.2 Standards [L.29.2.1; C.2.8.9.1.2]

We comply with the standards listed in the RFP and with other standards referenced by the listed standards as applicable.

2.2.8.8.2.3 Connectivity [L.29.2.1; C.2.8.9.1.3]

We comply with all connectivity instances listed in the RFP as applicable.

2.2.8.8.2.4 Technical Capabilities [L.29.2.1; C.2.8.9.1.4]

Agencies will receive IPSS that

Table 2.2.8-41

Section 2.2.8.8.1.1.

Table 2.2.8-41. DHS IPSS Technical Capabilities. GSA and agencies receive service

#	Technical Capability		Description
1.	DHS defined indicators desired effects		
2.	IPSS preactivation demonstration		
3.	DHS directed actions		
4.	Handle GFI up to TS/SCI including PII		
5.	GFI sharing near real-time		
6.	Commercially available capabilities and information		
7.	DHS-approved indicators and actions		
8.	Agency-specific mitigation		
9.	GFI non-disclosure		
10.	Access to approved participating agency federal system network traffic		
11.	Malicious traffic detection with contextual information		
12.	Emerging detection methods		
13.	Detection within encrypted traffic	Meets	

#	Technical Capability		Description
14.	Measures indicated in NIST Guide to Intrusion Detection and Prevention Systems		<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
15.	Safe server redirect		[REDACTED]
16.	Network traffic data capture and storage		[REDACTED]
17.	Traffic retention		[REDACTED]
18.	Application of US-CERT approved services		[REDACTED]
19.	Approved traffic segregation solution		[REDACTED]
20.	In-line service operation		<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
21.	Cyber-relevant speed operation		[REDACTED]
22.	Quarantined malware		[REDACTED]
23.	Operational capability demonstration		[REDACTED]
24.	Detection alerts		[REDACTED]
25.	Network traffic pattern assessments		<p>[REDACTED]</p> <p>[REDACTED]</p>

#	Technical Capability		Description
26.	Providing information over given time period		
27.	Appropriate disclosure		
28.	Testing and test results		
29.	Discovery notification to DHS		

2.2.8.8.2.5 Features [L.29.2.1; C.2.8.9.2]

Agencies receive established IPSS elements

Table 2.2.8-42

Section 2.2.8.8.1.1.

Table 2.2.8-42. IPSS Features. Agencies receive service

#	Feature		Description
1.	Classified email threat detection and countermeasures		
2.	Classified DNS threat detection and countermeasures		
3.	Additional counter-measures as specified by DHS		

2.2.8.8.2.6 Interfaces [L.29.2.1; C.2.8.9.3]

The AT&T IPSS is compatible with interfaces in RFP Section C.2.8.9.3, as applicable.

2.2.8.8.2.7 Performance Metrics [L.29.2.1; C.2.8.9.4]

The AT&T IPSS will meet performance metrics for IPSS as defined in a TO.

2.2.8.9 Software Defined Wide Area Network Service (SDWANS) [L.29.2.1; M.2.1; C.2.8.10]



2.2.8.9.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

2.2.8.9.1.1 Understanding [L.29.2.1(A); M.2.1(1)]

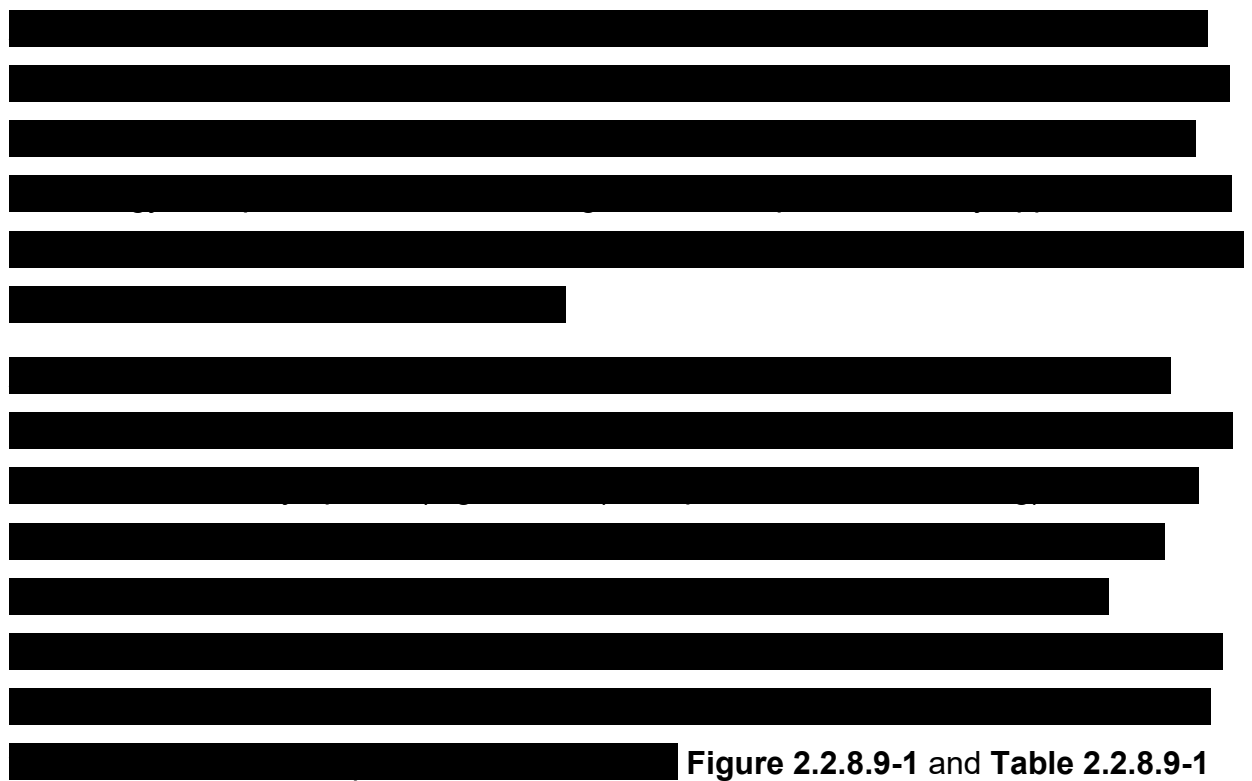


Figure 2.2.8.9-1 and Table 2.2.8.9-1
below.

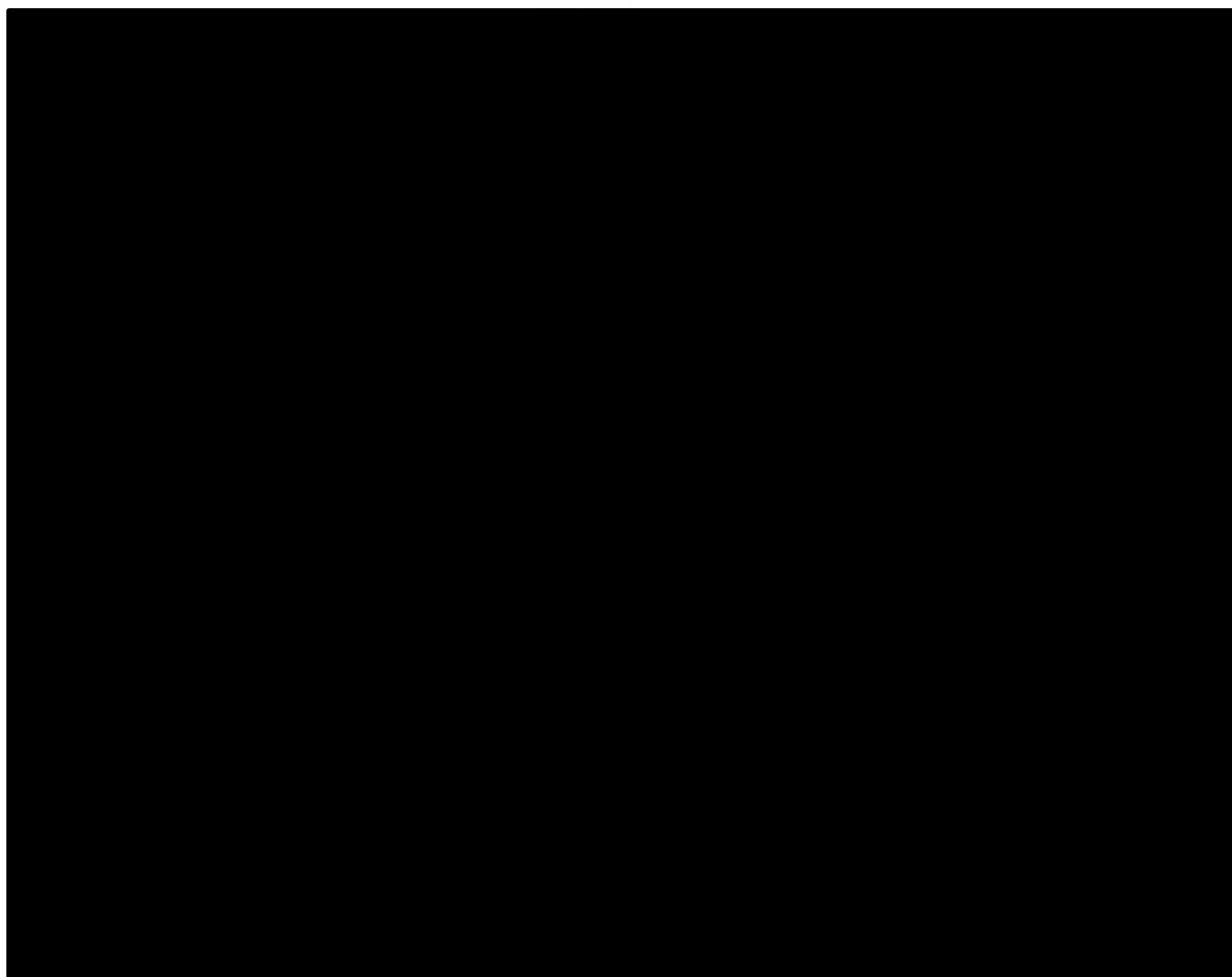


Figure 2.2.8.9-1. SDWANS Overview.

Table 2.2.8.9-1. SDWANS Overview Description.

Architectural Components	Description
Technical Components	
WAN edge devices	<ul style="list-style-type: none"> WAN edge devices are responsible for connecting the SD-WAN network to the Internet and other external networks. WAN edge devices are responsible for enforcing security policies and managing network traffic. WAN edge devices are responsible for managing the network's overall health and performance.
Controllers	<ul style="list-style-type: none"> Controllers are responsible for managing the network's overall health and performance. Controllers are responsible for enforcing security policies and managing network traffic. Controllers are responsible for connecting the SD-WAN network to the Internet and other external networks.



Architectural Components	Description
Orchestrator	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] vManage represents the user interface of the solution
Operational Components	
Topology policies	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Traffic flow policies	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Locally significant policies	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED] [REDACTED]
Service level agreement	<ul style="list-style-type: none"> [REDACTED]
Quality of Service	<ul style="list-style-type: none"> [REDACTED]
Network Components	
WAN Edge routers	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]
Access circuit	<ul style="list-style-type: none"> [REDACTED] [REDACTED] [REDACTED]

2.2.8.9.1.2 Quality of Services [L.29.2.1(B); M.2.1(2)]

Table 2.2.8.9-2.

Table 2.2.8.9-2. SDWANS Quality of Service.

Architectural Components	Description
Compliance	
Demonstrated compliance	<ul style="list-style-type: none">
Scalability	
Full mesh hub/spoke dynamic routing	<ul style="list-style-type: none">
Multicast	<ul style="list-style-type: none">
Reliability	
Infrastructure design	<ul style="list-style-type: none">
Forward Error Correction (FEC)/Packet dup	<ul style="list-style-type: none">
Network Transport	<ul style="list-style-type: none">
Resilience	
Monitoring	<ul style="list-style-type: none">
High Availability	<ul style="list-style-type: none">

2.2.8.9.1.3

See Section 1.3

2.2.8.9.1.4 Security [L.29.2.1(D); M.2.1(4)]

2.2.8.9.1.4.1 Service-Specific Requirements [M.2.1(4)(a); C.1.8.7.1]

Section 2.2.5.1.2.4. , Figure 2.2.5-2

Table 2.2.8.9-3

Table 2.2.8.9-3. SDWANS Service-Specific Security Capabilities.

Capability	Description
Encryption	
Network security	
Application security	

2.2.8.9.1.4.2 General Requirements [M.2.1(4)(b); C.1.8.7]

2.2.8.9.1.4.3 External Traffic Routing Requirements [M.2.1(4)(c); C.1.8.8(3); J.4]

Table 2.2.8.9-4

Table 2.2.8.9-4. Approach to External Traffic Routing Requirements.

Requirement	Compliance Description
Methodology for Identifying AT&T Participating Agency Traffic for Each Affected Service [M.2.1.4.c.i].	
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 [M.2.1.4.c.ii]	
Technical Approach to Notify DHS If Any Non-Participating Agency Traffic Will Be Redirected Through DHS EINSTEIN Enclaves [M.2.1.4.c.iii]	

Requirement	Compliance Description
Control Mechanisms to Ensure the Identification and Redirection of Participating Agency Traffic Cannot Be Inadvertently or Maliciously By-Passed [M.2.1.4.c.iv]	
Sensing and Control Mechanisms to Ensure the Redirection of Traffic is Failsafe [M.2.1.4.c.v]	
Location of AT&T Certified Facilities [M.2.1.4.c.vi]	
Availability of TS/SCI Cleared Personnel for “Smart-Hands” Service of DHS Supplied Equipment [M.2.1.4.c.vii]	
Instrumentation to Measure Transport SLA KPIs [M.2.1.4.c.viii]	

2.2.8.9.2 Technical Response for SDWANS [L.29.2.1; M.2.1]

2.2.8.9.2.1 Service Description and Functional Definition [L.29.2.1; C.2.8.10.1; C.2.8.10.1.1]

Table 2.2.8.9-5 Section

2.2.8.9.1.1.

Table 2.2.8.9-5.

Solution Element	Description
WAN Edge routers	
Maintenance	
Software	

2.2.8.9.2.2 Standards [L.29.2.1; C.2.8.10.1.2]

AT&T will comply with standards listed in the EIS Contract Section C.2.8.10.1.2, as well as those referenced by the listed standards as applicable.

2.2.8.9.2.3 Connectivity [L.29.2.1; C.2.8.10.1.3]

2.2.8.9.2.4 Technical Capabilities [L.29.2.1; C.2.8.10.1.4]

Table 2.2.8.9-6.

Table 2.2.8.9-6. SDWANS Technical Capabilities.

#	Technical Capability		Description
1.	Commercial broadband Internet service		
2a.	Secure IP-based virtual overlay network that uses IPSec tunnels		
2b.	Underlay physical networks		
2c.	End-to-end secure IPSec tunnels		
3a.	Define policies for application forwarding decisions		
3a) i.	Performance based routing for multi-homed nodes		
3a) ii. 1.	Latency tolerant applications vs latency sensitive applications		
3a) ii. 2.	Application priority		
3a) ii. 3.	Committed bandwidth		
4a.	uCPE/virtualized edge router automated configuration and policies		

2.2.8.9.2.5 Features [L.29.2.1; C.2.8.10.2]

Use or disclosure of data contained on this page is subject to the restriction on the title page of this document.

#	Feature		Description
5.	Virtual Trusted Internet Connection (vTIC)		
6.	Network-as-a-Service (NaaS)		

2.2.8.9.2.6 Interfaces [L.29.2.1; C.2.8.10.3]

2.2.8.9.2.7 Performance Metrics [L.29.2.1; C.2.8.10.4]

2.2.9 Service Area: Service Related Equipment [C.1.8.1]

2.2.9.1 Service Related Equipment [L.29.2.1; M.2.1; C.2.10]

Agencies will receive

The AT&T response for SRE addresses the requirements listed as mandatory in RFP Section C.2.10 and subordinate paragraphs. This response conforms to Q&A 263 in Amendment 1, which states: “The bulleted items in L.29.2.1 do not apply to SRE, Warranty Service, SRL and Cable and Wiring. The last sentence of L.29.2.1 provides direction for responding to optional services.” The directions at L.29.2.1 state: “For optional services, the offeror must address all requirements listed as mandatory within each optional service.”

2.2.9.1.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1; C.2.10; C.2.10.1]

To meet agency needs, AT&T offers SRE components similar or the same as those used to serve our commercial, enterprise customers. Deployment and life-cycle maintenance of SRE's will use many of the AT&T established and proven service models for customer premises infrastructure, and include hardware and materials that are incidental to the installation, operation and maintenance of EIS services.

EIS defines a government-specified method for agencies to purchase SRE required to connect to the EIS contractor services. The AT&T approach provides the service scope described in **Table 2.2.9-1**.

Table 2.2.9-1. SRE Service Approach. Agencies receive warranty service

Solution Element	Description
Responsive to TOs	
Incidental to service	
Only new equipment	
Proprietary technology	

AT&T will offer a catalog of SRE to provide service functionality according to specifications and to satisfy customer end-to-end networking needs. SRE's are the customer premises network, telephony, and IT infrastructure components required with certain EIS service offerings. SREs are similar in concept to the SEDs offered under the existing GSA Networkx contract.

2.2.9.1.2 Warranty Service [C.2.10.1]

AT&T warranty service meets all requirements as shown in **Table 2.2.9-2**.

Table 2.2.9-2. SRE Warranty Service. Agencies receive warranty service

Solution Element	Description
One-year minimum warrantee	

Solution Element	Description
Information to GSA	[REDACTED]
Responsiveness	[REDACTED]
Available POC	[REDACTED]
Warranty option	[REDACTED]

2.2.10 Service Area: Service Related Labor [L.29.2.1; M.2.1; C.1.8.1]

2.2.10.1 Service Related Labor [L.29.2.1; M.2.1; C.2.11]

Agencies will receive worldwide service related labor for construction, alteration, and repair that augment the full scope of services delivery and [REDACTED]

The AT&T response for SRL addresses the requirements listed as mandatory in RFP section C.2.11 and subordinate paragraphs. This response conforms to Q&A 263 in Amendment 1, which states: “The bulleted items in L.29.2.1 do not apply to SRE, Warranty Service, SRL and Cable and Wiring. The last sentence of L.29.2.1 provides direction for responding to optional services.” The directions at L.29.2.1 state: “For optional services, the offeror must address all requirements listed as mandatory within each optional service.”

2.2.10.1.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1]

In cases where agencies require labor to support services as defined in TOs, AT&T will provide service related labor at fixed hourly rates. Our resources support all of the required labor categories specified in RFP Section J.5. We offer labor for construction, alteration, and repair, as necessary, to offer a complete solution—deploying labor that is integral to, and necessary for, the effort defined in the TO.

2.2.11 Service Area: Cable and Wiring [C.1.8.1]

2.2.11.1 Cable and Wiring [L.29.2.1; M.2.1; C.2.12]

Agencies will receive cable and wiring services (CWS) globally that augment the full scope of EIS services that are proven on over [REDACTED]

The AT&T response for CWS addresses the requirements listed as mandatory in RFP section C.2.12 and subordinate paragraphs. This response conforms to Q&A 263 in Amendment 1, which states: “The bulleted items in L.29.2.1 do not apply to SRE, Warranty Service, SRL and Cable and Wiring. The last sentence of L.29.2.1 provides direction for responding to optional services.” The directions at L.29.2.1 state: “For optional services, the offeror must address all requirements listed as mandatory within each optional service.”

2.2.11.1.1 How AT&T Will Provide Proposed Services and Features [L.29.2.1; M.2.1; C.2.12]

AT&T will provide installation services for cable and wiring necessary to provide EIS telecommunication services across all service offerings. Our approach for these services is described in **Table 2.2.11-1**.

Table 2.2.11-1. Cable and Wiring Service Scope and Functional Capabilities. Agencies receive cable and wiring service proven by successful delivery on the current Networx contract to over 45 projects.

Solution Element	Description
Installation services	[REDACTED]
Providing connectivity	[REDACTED]
Site preparation	[REDACTED]
Warranty	[REDACTED]
Proprietary technology	[REDACTED]

2.3 Traffic Identification and Routing Policy [L.29(2)(c); L.29.2.3; M.2.1(4)(c);C.1.8.8(3)]

2.3.1 Detailed Technical Description [L.29.2.3; C.1.8.8]

The RFP requirements for this section are addressed in **Section 1.4** regarding security of AT&T proposed architecture. We provide in **Table 2.3-1** topic references to four relevant subsections within **Section 1.4**.

Table 2.3-1. Approach to Aggregation Service. Agencies receive services

Requirement	Reference
Detailed technical description [L.29.2.3; C.1.8.8]	
Design of AT&T aggregation service [L.29.2.3]	
Implementation of AT&T aggregation service [L.29.2.3]	
Operation of AT&T aggregation service [L.29.2.3]	

2.3.2 Technical Viability of AT&T's Aggregation Service [L.29.2.3(1)-L.2.9.2.3(8)]

The RFP requirements for this section are the same as those for previous **Section 1.4.3**. We provide in **Table 2.3-2** references to the eight relevant subsections within **Section 1.4.3**.

Table 2.3-2. Approach to Aggregation Service. Agencies receive services

Requirement	Reference
Methodology for identifying AT&T participating agency traffic for each affected service [L.29.2.3.1]	
Technical approach, for each affected service, to redirect all participating agency internet, extranet, and interagency traffic to DHS EINSTEIN enclaves, receive processed traffic from GFP within the DHS EINSTEIN enclave, and deliver traffic to its final destination [L.29.2.3.2]	
Technical approach to notify DHS if any nonparticipating agency traffic will be redirected through DHS EINSTEIN enclaves [L.29.2.3.3]	
Control mechanisms to ensure the identification and redirection of participating agency traffic cannot be inadvertently or maliciously bypassed [L.29.2.3.4]	
Sensing and control mechanisms to ensure the redirection of traffic is failsafe [L.29.2.3.5]	
Location of AT&T certified facilities [L.29.2.3.6]	
Availability of TS/SCI cleared personnel for Smart-Hands service of DHS supplied equipment [L.29.2.3.7]	
Instrumentation to measure transport SLA KPIs [L.29.2.3.8]	



General Services Administration (GSA)

Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

GS00Q17NSD3000

Appendix A — Risk Management Framework Plan

APPENDIX A — RISK MANAGEMENT FRAMEWORK PLAN [L.29(3)(A); L.29.2.2; L.11; C.1.8.7; C.1.8.7.4]

Ensurance of Delivery of System Security for the EIS Services [L.29.2.2; C.1.8.7; C.1.8.7.4]

To assist GSA in protecting the confidentiality of government information and to maintain the availability of the system, AT&T services delivered for EIS will be implemented and operated in accordance with a comprehensive Risk Management Framework (RMF). This approach to risk management is consistent with NIST Special Publication (SP) 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*. Our RMF is a risk-based approach to provide security for systems and services provided under this contract, and complies with the applicable IT security directives, standards, and policies.

AT&T applies the approach that risk is a measure of the extent to which an entity is threatened by a potential circumstance or event and a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of the occurrence of the event.

To manage and reduce risk to the lowest practical level, the AT&T RMF plan follows the six-step NIST RMF approach that includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The AT&T RMF plan follows the entire life cycle of a delivered service, beginning in the development phase through continuous monitoring and service decommissioning and removal of government information. Security of the EIS network and services architecture will adhere to all the general requirements described in EIS RFP Section C.1.8.7.

In addition, in accordance with requirements indicated in RFP Section C.2.8.5.5:

- AT&T will comply with all security A&A requirements mandated by federal laws, directives and policies, including making available any documentation, physical access, and logical access needed to support this requirement.
- AT&T will confirm that proper privacy and security safeguards are adhered to in accordance with the FAR Part 52.239-1.

- AT&T will confirm, where appropriate, the implementation of the requirements identified in the FAR (see Section I, 52.224-1, “Privacy Act Notification” and FAR 52.224-2, “Privacy Act.”)
- AT&T will cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the federal government’s agent.
- AT&T will afford the government logical and physical access to the contractor’s facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request.

A-1 The AT&T Risk Management Framework Plan [C.1.8.7; C.1.8.7.4]

The AT&T RMF plan provides the following:

- Promotes the concept of near real-time risk management through the implementation of robust continuous monitoring processes supporting ongoing authorization as applicable;
- Applies automation to provide system operations teams and AT&T senior leaders with the necessary information to make risk-based decisions on system operations;
- Integrates information security into the enterprise architecture and system development life cycle;
- Establishes responsibility and accountability for security controls implemented in AT&T service infrastructure and inherited by systems, such as common controls across shared management infrastructure;
- Provides the methodology and guidance to integrate required security controls into AT&T enterprise architecture and system development life cycle processes, providing the government with services; and
- Provides comprehensive protections against threats to Confidentiality, Integrity or Availability.

As shown in **Figure A-1-1**, the Risk Management Framework (RMF) overlays the standard system development life cycle phases – Initiate, Design, Implement, Operations & Maintenance, and Dispose. We implement, assess, and monitor ongoing compliance with the applicable baseline security requirements specified in NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for moderate- impact systems and other related GSA directives and

guides. Our RMF approach is based on the guidance in NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* and GSA IT Security Procedural Guide 06-30, *Managing Enterprise Risk*. The processes and deliverables of the AT&T RMF Plan consist of the following:

- Follows the GSA or agency Task Order (TO) for system impact categorization and documents the security categorization in the Service System Security Plan (SSP). (NIST SP 800-37, Section 3.1, *RMF Step 1 – Categorize Information System*)
- Describes each service infrastructure, including system boundary, in the SSP. The AT&T RMF defines an information system boundary based on several factors: (NIST SP 800-37, Section 2.3, *Information System Boundaries*)
 - The EIS defines a number of services that a vendor shall provide. If any of those services support similar objectives or functions, such as basic voice and toll free services, we could consider those services within the same system boundary.
 - Systems or service infrastructure that use common operating components. Examples of common components are network hardware/software or transport, IP backbone, and VLAN Range.
 - Transmission of government-sensitive data.
- Registers the systems that support the delivered service with appropriate AT&T organizational program/management offices for oversight and system owner identification.

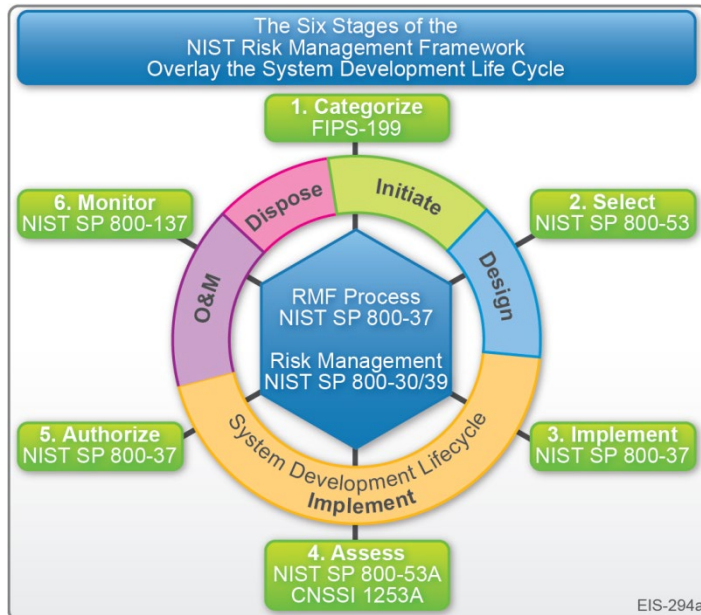


Figure A-1-1. AT&T RMF Life Cycle. Properly implemented, the RMF synchronizes information security with system development and maintenance, resulting in more thorough and economical compliance throughout the life cycle.

- Identifies any common controls that are inherited from systems outside the service infrastructure system boundary and document them in the SSP. (NIST SP 800-37, Section 2.4, *Security Control Allocation*)
- Verifies the security controls from the NIST 800-53, Rev. 4, baseline for a moderate-impact system and any additional controls required by GSA and/or agency provided TO needed to address specific information security risks and document them in the SSP. (NIST SP 800-37, Section 3.2, *RMF Step 2 – Select Security Controls*). If a Cloud solution is used, we will categorize the security system at a minimum of Moderate Impact Level and provide the appropriate deliverables in the security package as identified at www.FedRAMP.gov. If a Cloud solution is used, we will categorize the security system at a minimum of Moderate Impact Level and provide the appropriate deliverables in the security package as identified at www.FedRAMP.gov.
- Develops a continuous monitoring strategy for monitoring security control effectiveness and any proposed/actual changes to the service infrastructure and its operating environment. The AT&T continuous monitoring strategy reflects, and is consistent with, the NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* and the GSA organizational continuous monitoring strategy and program as described in GSA IT Security Procedural Guide: *Information Security Continuous Monitoring Strategy*, CIO-IT Security-12-66. (NIST SP 800-37, Section 3.2, *RMF Step 2 – Select Security Controls/Monitoring Strategy*)
- Implements the security controls specified in the SSP. (NIST SP 800-37, Section 3.3, *RMF Step 3 – Implement Security Controls*)
- If required by an agency TO, submit a service SSP and other required documentation and artifacts of system that demonstrate adherence to the required NIST, GSA, and agency-specific security controls to the agency's Authorizing Official (AO) for review and approval.
- Documents the security controls implementation in the SSP, providing a functional description of how each control is or will be implemented, including planned inputs,

expected behavior, and expected outputs. (NIST SP 800-37, Section 3.3, *RMF Step 3 – Implement Security Controls/Security Control Documentation*)

- Develops a Security Assessment Plan (SAP) for testing the service infrastructure to verify that the required controls specified in the approved SSP are implemented as described and providing the appropriate level of risk management. The SAP describes what technologies and sub-systems are to be assessed and from this the actual assessment will determine if there are any vulnerabilities or weaknesses of a system's technologies or sub-systems when tested against the applicable security controls. For systems that are required to operate under an authorization specified in a TO, we will submit the SAP to the AO or their designee for review and approval. (NIST SP 800-37, Section 3.4, *RMF Step 4 – Assess Security Controls/Assessment Preparation*)
- Executes the SAP to assess the effectiveness of service infrastructure security controls. The AT&T program Information Systems Security Officer (ISSO) or for systems required to operate under a TO specified authorization, an agency AO or designated representative analyzes the SAP testing results to determine the effectiveness of the security controls for a given system. From that analysis, the ISSO, agency AO, or designated representative decides whether or not to grant the system the authority to operate. (NIST SP 800-37, Section 3.4, *RMF Step 4 – Assess Security Controls/Security Control Assessment*)

Where applicable for service infrastructure that has an agency TO authorization requirement, the AT&T RMF outlines how AT&T works with an independent third party assessor. The assessor can be either contracted by AT&T or an agency designee to perform the required testing of the service infrastructure security controls.

- Prepares a security assessment report (SAR) to document any issues, findings, and recommendations from the security control assessment. (NIST SP 800-37, Section 3.4, *RMF Step 4 – Assess Security Controls/Security Control Assessment*)
- Conducts initial remediation actions based on the findings and recommendations in the SAR and reassesses remediated control(s), as appropriate. (NIST SP 800-37, Section 3.4, *RMF Step 4 – Assess Security Controls/Security Control Assessment Remediation*)

- Prepares a Plan of Action and Milestones (POA&M) based on the SAR findings and recommendations, excluding any remediation actions taken. For service infrastructure that is operating under an agency authorization, the government provides final determination of open finding risk rating (critical/high, moderate, or low).
(NISTSP 800-37, Section 3.5, *RMF Step 5 – Authorize Information System Plan of Action and Milestones*)
- For service infrastructure operating under an agency authorization as stated in a TO, the following action is provided per the AT&T RMF plan: (NIST SP 800-37, Section 3.5, *RMF Step 5 – Authorize Information System Security Authorization Package*):
 - Assembles the security authorization package and submits to the AO for authorization, where the level of effort is based on a system's NIST FIPS Pub 199 categorization.

The basic authorization package consists of the following deliverables:

- SSP (in accordance with NIST SP 800-18, Rev 1) with required appendices;
- SAR; and
- POA&M.

If the service infrastructure inherits common controls, then we include either the authorization package for the common controls or a reference to the documentation. If any inherited common controls are provided by an external provider this information is included in the AO to support the authorization decision.

Also included with the authorization package are SSP appendices and additional documentation as specified in the TO, per NIST and GSA guidelines:

- Applicable Interconnection Security Agreements (ISAs);
- Control Tailoring Workbook;
- Rules of Behavior (RoB);
- System Inventory, as a section in the System Design Document (SDD);
- Contingency Plan (CP), including the Disaster Recovery Plan (DRP) and Business Impact Assessment (BIA);
- Contingency Plan Test Plan (CPTP);
- Privacy Impact Assessment (PIA);

- Configuration Management Plan (CMP) with system baseline configuration and BSS configuration settings;
- Incident Response Plan (IRP);
- Incident Response Test Report (IRTR);
- Continuous Monitoring Plan (CMP);
- Vulnerability scan outputs, as required; and
- Code Review Report, as required.

AT&T will make available any documentation, physical access, and logical access needed to support all Assessment and Authorization (A&A) requirements mandated by federal laws, directives and policies.

Upon placing a service into operation or when a TO requires an authorization and after the AO grants the service an Authorization to Operate (ATO), the system moves into *RMF Plan, Step 6, Monitor Security Controls*, the Continuous Monitoring of Security Controls of AT&T System with a Continuous Monitoring Plan.

The on-going security monitoring activities consist of the following:

- Assesses the security impact of proposed or actual changes to the Service Infrastructure and its operating environment;
- Annually assesses a subset of the Service Infrastructure operational policy security controls consistent with the continuous monitoring plan;
- Remediates vulnerabilities based on the results of the ongoing monitoring activities and risk assessment, as prescribed and tracked through the POA&M;
- Maintains the SSP, SAR, and POA&M; and
- Prepares and submits system security status reports, per the continuous monitoring plan, to AT&T leadership and the agency AO when the service infrastructure is under an agency authorization.

The AT&T RMF is a comprehensive plan designed to deliver services with infrastructure that is designed, implemented, operated, and monitored to provide the government with services that are verified secure and continuously reviewed for strict adherence to GSA and agency security requirements. (NIST SP 800-37, Section 3.6, *RMF Step 6 – Monitor Security Controls*)

A-2 The AT&T RMF Plan Management and Oversight [C.1.8.7]

The AT&T RMF plan is managed by the AT&T Information Assurance (IA) organization. The IA organization provides independent oversight of the system and service infrastructure development and operations organizations at AT&T. The IA organization's RMF-defined functions include the following major tasks: (NIST SP 800-37, Section 1.2 *Purpose and Applicability*)

- Selects the GSA, agency specific, and AT&T security controls that systems and service infrastructure supporting the EIS follow based on the RMF plan, GSA guidance of risk determination, and/or agency specification. The IA organization provides guidance to all technical, operational, and managerial staff on how each security controls is be implemented.
- Verifies that the technical, operational, and managerial organizations document how the selected controls are implemented and followed. This documentation includes the SSP, SSP appendices, technical system descriptions, personnel suitability verification processes, and other artifacts used as reference to demonstrate adherence to an accepted system risk profile.
- Test and/or support an agency's independent assessor to perform preproduction testing of all technical, operational, and managerial security controls verifying compliance prior to providing service to the government.
- Reviews and verifies that all personnel supporting systems and service infrastructure hold the appropriate credentials and suitability to access restricted government information.
- Performs system lifecycle continuous monitoring of the technical, operational, and managerial security controls verifying that the system and service infrastructure is operated in accordance with the approved risk profile. This monitoring includes monthly testing and quarterly POA&M reporting of technical control implementation, verifying adherence to operational policies, and reviewing managerial oversight per NIST and GSA guidelines. The continuous monitoring performed by the IA organization verifies that the infrastructure is in constant compliance with all required security controls and reports on any identified deficiencies to senior leadership and, if required, to agency AO using the POA&M as the reporting method.

- Works together with the agency AO, where service infrastructure operates under an agency ATO on required reauthorization deliverables. The AT&T RFP plan and the Continuous Monitoring Plan provides support for continuous compliance to allow for continuing authorization when an agency so chooses. This is accomplished by providing artifacts quarterly and annually that demonstrate verification of compliance, reducing the cost of Assessment and Authorization with an assessor over three years.
- Engages in disaster recovery testing, incident response testing, and security events mitigation.

A-2.1 IA Organization Team Alignment in Support of the RMF Plan [C.1.8.7]

The IA organization is a member of the AT&T Compliance and Governance organization in the Services Assurance division. The IA organization is independent of the direct reporting chain from Service Development, Service Operations management, and customer Program Management organizations. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The ISSOs have direct working relationships with all system and service infrastructure owners and attend project meetings to facilitate communications, expectations, system status, change control, patching, planned upgrades, and incident engagement.

Figure A-2.1-1 depicts the AT&T IA Organization. (NIST SP 800-37, Section 2.2, *System Development Life Cycle*)

A-2.2 IA Organization Team Alignment in Support of the RMF Plan [C.1.8.7; C.1.8.7.7]

The IA ISSO assigned to each system has the primary oversight to execute the RMF plan for the system. When developing the infrastructure supporting the EIS services, the ISSO follows applicable NIST and OMB guidance on the selection and implementation of the security controls. The ISSO follows the specific guidance below for providing the

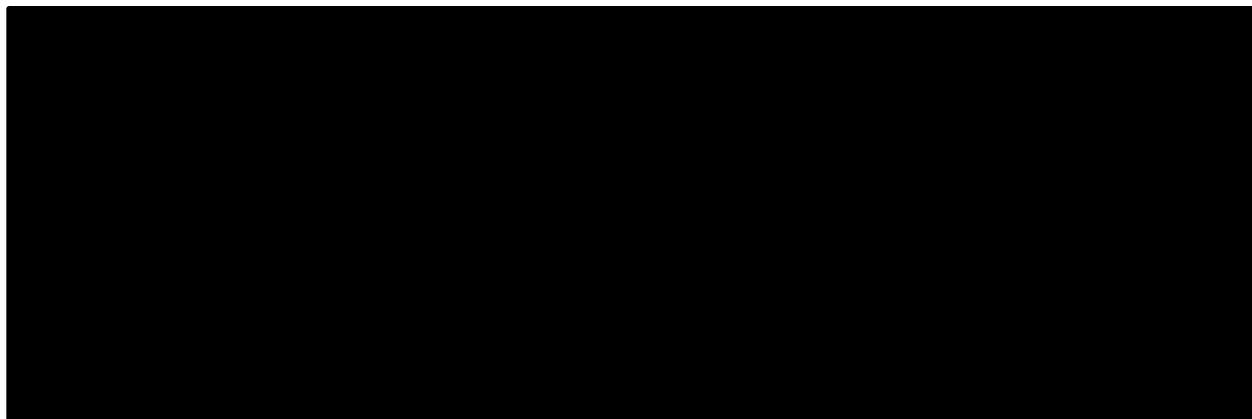


Figure A-2.1-1. AT&T IA Organization.

implementation and operation teams on the execution of specific security controls. The AT&T RMF plan places the NIST SP 800-53, Rev. 4, controls, GSA and agency specific security controls, and AT&T corporate controls into three logical categories for tracking and management oversight. These categories are management controls, operational controls, and technical controls. Each of these categories are used to identify which AT&T organizations assign a resource to work with the ISSO to implement and verify control implementation compliance.

The implementation of the controls, while broken down into categories of managerial, operational, and technical controls for a specific system to provide clear and direct ownership, also follow the guidance for the types of security controls provided in NIST SP 800-37, Section 2.4, *Security Control Allocation*. AT&T follows the concept of identifying controls as they are implemented across the organization as:

- **System-specific Controls:** controls that provide a security capability for a designated information system.
- **Common Controls:** controls that provide a security capability for multiple information systems.
- **Hybrid Controls:** controls that have both system-specific and common characteristics.

AT&T follows NIST guidance to identify common or inherited controls and the senior management and operational resources responsible to implement and operate the common controls. This is accomplished in accordance to the applicable NIST SP 800-53, Rev. 4, security control guidance and consistence with the risk profile of specific

systems that use the common controls. (NIST SP 800-37, Section 3.0, *Executing the Risk Management Framework Tasks*)

- **Management Controls:** Management controls are actions taken to manage a system's development, maintenance, and use. This includes system-specific policies, procedures, assignment of individual roles and responsibilities, and rules of behavior. These controls are the overriding practices that must be followed so the systems operate as expected. (NIST SP 800-37, Section 3.3, *RMF Step 3 – Implement Security Controls*)
- **Operational Controls:** The operational controls address security mechanisms that focus on methods that are primarily implemented by people, as opposed to those implemented by systems. The methods often require technical or specialized expertise and often rely on management activities as well as technical controls. **Table A-2.2-1** describes the types of control topics associated with operational controls. (NIST SP 800-37, Section 3.3, *RMF Step 3 – Implement Security Controls*)

Table A-2.2-1. Operational Control Topics. *Operational controls consist of the following requirements.*

Control Requirement	Description
Personnel security	<ul style="list-style-type: none"> ■ These controls provide guidance on restricting access to appropriately credentialed and suitable personnel. The controls also provide guidance on applying the concept of Least Privilege to Role Base assignments that restricts access to no more functionality than each person needs to execute their assigned role, as outlined in the NIST guidance. Personnel security also includes log audit controls to trace user activity back to each use. Finally the controls establishes procedures for maintaining the security of the system when personnel who have had access granted no longer require access. ■ The depth, breadth, and rigor of the personnel security controls required for a system vary depending on numerous factors, including the system's sensitivity and, where applicable, the authorizing agency's unique requirements. The following subsections represent a scenario that somewhat typifies the Personnel Security section of an AT&T security plan. ■ It is important to note that the AT&T RMF plan is used as a minimum guideline and is a starting process that will be customized for any system for which an agency contracts for support under EIS. Like all other security plan sections, it will be customized to reflect the requirements of a specific system in a specific agency as required when specified in a TO.
Personnel security management	<ul style="list-style-type: none"> ■ The AT&T RMF Plan for EIS provides guidance on the personnel security management baseline to meet GSA requirements for delivering services that are implemented and operated in accordance with the NIST SP 800-53, Rev. 4 Moderate Impact Baseline security controls operated with personnel who have been granted HSPD-12 suitability at the appropriate Position of Public Trust Level based on their Role, and in accordance with FAR Part 52.204-9. ■ AT&T will designate an individual whose role includes coordinating the aspects of the task order that pertain to obtaining and maintaining security clearances at the appropriate levels for AT&T personnel. The individual's responsibilities will include such activities as obtaining and maintaining security clearances, if needed, and suitability, and related coordination with the agency, and monitoring approvals for persons with physical access to sensitive facilities. ■ The AT&T security office has the experience and knowledge to manage any level of required personnel credentials and currently initiates/processes an average of 56 new security credentials per month.

Control Requirement	Description
Sensitivity of positions	<ul style="list-style-type: none"> The sensitivity of positions that require system access will depend on the classification level of the system. There are expected to be two classifications of users, 1) privileged administrative users, such as system administrators, and 2) generic users. Work performed under EIS task order(s) may fall within one or more of the risk categories defined below. Therefore, AT&T personnel will undergo background investigations commensurate with the risk factor associated with the duties of each position. <ul style="list-style-type: none"> High Risk positions have the potential for exceptionally serious impact involving duties especially critical to the system-owning agency. These may include computer positions responsible for planning, directing, and implementing the system's security program; directing, planning, and designing the system, including the hardware and software; or accessing the system during its operation or maintenance in a way that would enable them to cause grave damage or realize significant personal gain. Moderate Risk positions are sensitive positions that have the potential for moderate to serious impact involving duties very important to the system-owning agency. These may include computer positions of a lesser degree of risk than seen in High Risk positions, as defined in OMB Circular A-130, Appendix III. Low Risk positions are non-sensitive positions that do not fall into either of the preceding categories and includes those positions with potential for impact involving duties of limited relation to the system-owning agency's mission.
Required background investigations	<ul style="list-style-type: none"> Background investigations will be conducted and favorably adjudicated, as applicable, for AT&T personnel before work commences. Typical minimum pre-appointment investigative requirements are as follows: <ul style="list-style-type: none"> High Risk positions may require a Limited Background Investigation (LBI), which consists of a personal subject interview, National Agency Check (NAC), credit history check, written inquiries, record searches covering the preceding five years, and personal interviews covering specific areas during the most recent three year period. Moderate Risk positions may require a National Agency Check and Inquiries (NACI), which consists of written inquiries and record searches covering specific areas of a subject's background during the preceding five years. Low Risk positions may require a Federal Bureau of Investigation (FBI) Name and Fingerprint check.
Pre-appointment background investigation waivers	<ul style="list-style-type: none"> Depending upon the client agency's requirements for the task order, the agency may be unable to wait for an entire background investigation to be completed. In such cases, it is common for a pre-appointment background investigation waiver to be granted by the authorizing agency. The extent of the background investigation needed to qualify for waivers varies by agency, system sensitivity, and position sensitivity. Typical waiver requirements are as follows: <ul style="list-style-type: none"> High Risk positions may require a successful NCIC check, vouchering of previous two employers, and a favorable review of forms submitted. Moderate Risk positions may require a favorable NCIC check and a favorable review of forms submitted. Low Risk positions may require a favorable NCIC check.
Required security forms	<ul style="list-style-type: none"> AT&T employees holding sensitive positions supporting federal agency systems, requiring HSPD-12 compliance, will complete the following forms: <ul style="list-style-type: none"> Applicant Fingerprint Card (FD-258) – two sets per applicant; and Questionnaire for Non-Sensitive Positions (SF-85), or Questionnaire for Public Trust Positions (SF-85 P). AT&T currently has over 3,000 cleared personnel. All AT&T IA personnel have been granted Secret clearances as a minimum; many possess Top Secret clearances; and several have higher levels.
Operational access controls	<ul style="list-style-type: none"> Access to an EIS system will be granted based upon the individual's assigned responsibilities with each user restricted to the minimum level of access necessary to perform their assigned duties. When possible, assignments to support critical functions will follow the principal separation of duty and will be divided among different individuals. If impractical, variations from this requirement will be justified and documented. This division or separation of duties will be established and maintained through access controls. Whenever possible,

Control Requirement	Description
	<p>administrator access shall be granted through user accounts rather than through root access.</p> <ul style="list-style-type: none"> Assignment of user privileges will follow the client agency's protocols for requesting, establishing, issuing, and closing user accounts. With ISSO oversight, the AT&T project manager or designee will provide oversight for access requests and approvals. AT&T will develop standard access control documentation that will be used to document access requests, justifications, and approvals for all systems. In addition, AT&T personnel assigned to an EIS task order will comply with the client agency's security policies and procedures, sign the rules of behavior, and follow the procedures developed for the operation and maintenance of the EIS system.
Holding users responsible for their actions	<ul style="list-style-type: none"> Two mechanisms will be in place for holding users responsible for their system-related actions: <ul style="list-style-type: none"> A Rules of Behavior (ROB) document is created for all systems and will be customized for any TO specific contracted system. The ROB is issued to all parties with physical and/or logical access to the network. Each person will sign a copy of the rules to acknowledge receipt and the project manager or designee will maintain the signed documents. The security audit capability and processes described below under Audit Trails will be implemented and maintained. Each system user will have their own account with a unique login ID and password. All security-related user activities will be logged. Each user will have a unique account creating an audit trail of each user's activities. As discussed in the Audit Trails section designated personnel will be responsible for periodically reviewing the administrator activity logs to identify any suspicious activity.
Friendly and unfriendly termination procedures	<ul style="list-style-type: none"> Upon termination or transfer of personnel from duties related to the contracted system environment, regardless if friendly or unfriendly, the ISSO has oversight for the process that requires the AT&T project manager or designee to request and verify that system access has been terminated. Judgment will be exercised in deciding upon the timing of terminating access. In the case of unfriendly terminations, system access will be terminated immediately. If an employee is to be fired, system access will be removed just before or at the same time the employee is notified of dismissal. When an employee gives notice of resignation and is suspected that it may be on unfriendly terms, system access will be terminated immediately. As part of the AT&T employee's exit interview, or at an earlier time if appropriate, the departing employee will be briefed on their responsibilities for confidentiality and privacy with respect to EIS task orders. Explicit direction will be given relative to what information, if any, is allowed to be disclosed. At the employee's exit interview, or at an earlier time, all tangible access tools, such as authentication tokens and key cards for facility doors, will be retrieved and accounted for. In the case of an unfriendly termination, cipher lock combinations will be changed, and keyed locks will be re-keyed upon the employee's departure.
Physical and environmental protection	<ul style="list-style-type: none"> The AT&T RMF plan will provide the following controls for each physical site where system devices, media, or other resources are housed in accordance with the corresponding NIST guidelines: <ul style="list-style-type: none"> Site plans detailing responses to emergencies for IT facilities. Annual reviews of physical security measures. Controlled physical access through the use of guards, identification badges, or entry devices such as key cards or biometrics. Keys or other access devices required to enter these sites, including data center(s), computer room(s), and tape/media libraries. Properly-secured keys or other entry devices that are not issued. A specific EIS task order will specify where and how these devices are secured and the individual(s) responsible for maintaining and issuing entry devices. Cipher lock entry codes will be changed periodically. Frequency will be defined in the SSP for each system where cipher locks are used. The schedule and off-schedule times at which codes are changed and the individual(s) responsible for ensuring that codes are changed as specified.

Control Requirement	Description
	<ul style="list-style-type: none"> — Authentication of visitors, contractors, and maintenance personnel who may access these sites. Authentication is done through the use of preplanned appointments and identification checks. — A procedure for signing in and escorting site visitors. A register is maintained that includes the names of the visitor and the person authorizing the visit, visitor's signature, date, and time-in and time-out. — Emergency exit and re-entry procedures to ensure only authorized personnel can re-enter after fire drills and any other similar mass departure/re-entry of the site. — System cabling and other communications equipment closets are physically secured to prevent unauthorized access. — Physical access to routers, switches, telephony gateways, routers, and other sensitive equipment is restricted to authorized personnel. — All perimeter walls and firewalls extend from the structural floor to the structural ceiling. — Interior and exterior windows do not open into a non-secured area. — Environmental protection for IT systems. The means of providing the protection will be documented. — Appropriate fire suppression and prevention devices are installed and properly functioning. — Reviews for fire ignition sources such as; failures of electronic devices or wiring, improperly stored materials, and the possibility of arson are performed in accordance with each AT&T operations facility and documented fire code procedures. — Cables leaving and entering the site installed with fire stops. — The temperature and humidity within the facility monitored and controlled to provide an operational environment that conforms to the manufacturer's specifications. — Heating and air-conditioning systems are maintained regularly. — Redundant air-cooling system for the site(s) are provided. — Building plumbing lines are identified and documented. — Reviews of electric power distribution, heating plants, water, sewage, and other utilities are conducted. — Power circuits are clearly identified, dedicated, and meet equipment manufacturer's amperage requirements. — Equipment that is grounded with American Wire Gauge (AWG) #6, meets manufacturer's specifications, and complies with local electrical code. — Uninterruptible power supply(s) (UPS) or backup generator(s) are available to support the system in the event of AC power failure. The UPS or generator(s) will provide a minimum of one hour of power. — Equipment cabinet doors that remain locked. — Controls to mitigate effects of disasters such as floods and earthquakes. — Network administration terminals equipped with the following safeguards: physically located to minimize unauthorized access or viewing; password control and password aging features invoked; timed auto logoff enabled, and protection from unauthorized use. — A risk analysis that considers additional environmental and physical controls for facilities that support large-scale IT operations, such as telecommunication facilities.
Production input/output controls	<ul style="list-style-type: none"> ■ The production input/output controls maintain the security posture of a system's live processing environment and appropriately distribute its data. These controls include help desk and other user support and are used for marking, handling, processing, storage, and disposal of input and output information and media. These controls are also used for labeling and distribution procedures for the input and output information and media. These controls include the mechanisms used to monitor installation and updates to the production environment.
Marking and storing devices and media	<ul style="list-style-type: none"> ■ AT&T protects system devices and electronic media by marking them in accordance with the system's sensitivity to the highest classification level authorized (e.g., Limited Official Use). System devices contain external classification markings authorizing the level of information that can be processed. Data is not stored on electronic media that cannot be adequately secured against unauthorized access.

Control Requirement	Description
Device and media disposal	<ul style="list-style-type: none"> System devices that have processed, stored, or transmitted sensitive information will not be released from system control until the equipment is sanitized and all stored information has been cleared. For sensitive information, the sanitization method will be approved by the client agency and documented in the customized security plan. If any system IT equipment is maintained under warranty contracts, the contracts will include stipulations that equipment removed from its hosting site will be sanitized before its removal. When no longer required for system support, IT storage media to be re-utilized for unrelated system purposes will be overwritten with software and protected consistent with the data sensitivity and/or at the highest classification level at which they were previously used. If the system processes, stores, or transmits classified data, then classified media will be disposed of in accordance with measures established by the National Security Agency (NSA) and the required disposal procedures of the client agency. Official electronic records will be properly disposed of and if appropriate archived. AT&T will identify any official electronic records related to the system and the approved disposal/archive procedures to be followed. The EIS Security Manager or designee will maintain records regarding all aspects of the implementation of disposal actions and verify the device or media was sanitized in accordance with NIST guidelines.
Monitor the production environment	<ul style="list-style-type: none"> Production, input/output controls include the mechanisms used to monitor installation and updates to the production environment. A System Test & Evaluation (ST&E) will be developed and executed, either by AT&T or by the agency's designated assessor for systems operated under an authorization as specified in the TO. The ST&E will validate that security requirements for contracted systems and service infrastructure for EIS services are satisfied. The ST&E will test controls as prescribed as well as compliance with secure operating system configuration requirements tested using one or more automated security scanning tools. As part of the ST&E the system will be reviewed to identify and eliminate unnecessary services, ports, and protocols. This review will occur on an annual basis or within six months after there is a significant change to the environment that alters the in-place assessed risk. The system will be reviewed annually or within six months after there is a significant change to the environment that alters the in-place assessed risk for known vulnerabilities and software patches will be installed. AT&T will specify the process by which the system will be reviewed including schedule, tools, methods, and responsible personnel. AT&T will also specify procedures for identifying, downloading, testing, and applying patches, service packs, and hot-fixes. The RMF plan requires that the use of any copyrighted software will be documented. Shareware and personally-owned software/equipment will require a waiver and will be documented. AT&T will include procedures under which any copyrighted software will be used in compliance with applicable copyright laws and will be incorporated into the system's life cycle management process. Other system configuration requirements are as follows: <ul style="list-style-type: none"> Laptops and mobile computing devices (including personal digital assistants [PDAs]) approved for processing sensitive information will not be connected to networks or systems unless the network or system is designed for that functionality. The devices will employ virus protection software and encryption technology. Automatically forwarding e-mail regardless of the forwarding method employed either to the system or through the system if it is a network, is forbidden unless the ISSO or, for services under a TO required authorization, the agency AO grants a waiver.
Contingency planning	<ul style="list-style-type: none"> Critical EIS services configurations, government sensitive data, and information generated and stored at AT&T EIS facilities will have a NIST compliant contingency plan in place throughout the length of the EIS contract period to facilitate continuity of system functions in the event of disruption in computer operations. These contingency plans, also referred to as disaster recovery plans or business recovery plans, will include steps to be taken to ensure preparedness including near real-time mirrored back-up of all servers at off-site locations and plans for timely response after a disruption. This process will be applied to systems that support critical EIS services and databases.

Control Requirement	Description
Continuity of operations plans	<ul style="list-style-type: none"> Three essential contingency planning activities will be combined to provide for plan related testing, training, and management approval. The plan will be tested and revised as necessary based on the testing. The plan will be tested using the tabletop approach. Using this approach, all personnel expected to implement any part of the plan will be assembled. Using a facilitated workshop methodology the assembled personnel will walk through multiple contingency scenarios validating the steps described in the plan. While the plan may require revision based on the testing, the individuals responsible for executing the plan will have been trained in their responsibilities by participating in the testing scenarios. Additionally, the approval of the key affected parties will be gained through the process. After revisal and approval from the system ISSO, the plan will be distributed to the personnel responsible for executing the plan. Once implemented, the plan will be tested annually or within six months after a significant change to the environment that alters the in-place assessed risk of the affected system.
Backup and off-site storage	<ul style="list-style-type: none"> Day-to-day security operations and administration will include performing regularly scheduled software backups and managing backup media. Recent software and data backups will be essential if disaster recovery is required regardless if it is natural or intentional. Duplicate backup media is stored off site, in accordance with NIST guidelines, to minimize the risk of being damaged or destroyed with the production environment.
Hardware and system software maintenance and repair	<ul style="list-style-type: none"> AT&T will develop on-site and off-site maintenance procedures. The procedures will include restrictions on who may perform maintenance and repair activities, guidelines and procedures for escorting maintenance personnel who need to work in restricted areas, and guidelines and procedures for securing devices or removable media that must be removed from the site. The capabilities to add, change, or remove system devices, dial-up connections, and network addresses and protocols or to remove or alter programs will be restricted to authorized personnel, as described in the <i>Personnel Security</i> and <i>Logical Access Controls</i> sections.
Hardware and system software configuration management	<ul style="list-style-type: none"> A configuration management process will be in place and documented to maintain control of system changes and to provide a current history of system change. AT&T will prepare a system configuration management plan. The plan will identify the personnel responsible for system configuration management as well as the guidance and procedures for configuration management. In accordance with NIST guidelines, AT&T will address the following requirements: <ul style="list-style-type: none"> Software change request forms to document requests and related approvals; Review, evaluation, and approval of all documentation, hardware, software, and firmware change requests before changes occur; Document and archive authorizations for all modifications; An impact analysis to determine the effect of proposed changes on existing security controls, including required training needed to implement the control; Procedures for testing all changes before modifying the accredited production system so that new information security vulnerabilities are not introduced into the operational environment; Revise approvals, after testing and documentation, to migrate changes into the production environment; and Emergency change procedures and the personnel authorized to approve an emergency change. Emergency changes will be documented and approved by management, either prior to the change or after the fact. The configuration management plan also will specify procedures and documentation requirements for maintaining version control over production software and hardware, labeling and inventorying software, and distributing and implementing new or revised software.
Integrity controls	<ul style="list-style-type: none"> Integrity controls protect the system and the data it processes, stores, and/or transmits from accidental or malicious alteration or destruction and provide assurance to the end user that the information meets expectations about its quality and that it has not been altered. Validation controls are tests and evaluations used to determine compliance with security specifications and requirements. The system security requirements and controls that fall within this category are described in the following sections.

Control Requirement	Description
Virus control	<ul style="list-style-type: none"> ■ AT&T understands anti-virus software is most effective when kept current. Therefore, the ISSO will verify that procedures for maintaining current anti-virus signatures are defined and implemented. ■ AT&T emphasizes the protection of the support systems from viruses, worms, and other disruptive influences to maintain data integrity and availability. In support of this effort, AT&T takes the following steps with individual and corporate access equipment to service providing systems: <ul style="list-style-type: none"> — Install the latest version of the corporate licensed anti-virus software designated by Network Security for AT&T use; — Options of automated anti-virus software to maintain current protections are not disabled or modified; — Run the anti-virus software on all local drives and all removable media maintained by the user; — Scan all network shares owned by the user; — Scan all files that have been downloaded or copied from email messages or the Internet; — Perform regular back-ups (preventing all data from being lost in case of pervasive virus or catastrophic attack); and — Use only company authorized (i.e., purchased, owned, leased, or management-approved) software on company computers.
Message integrity	<ul style="list-style-type: none"> ■ AT&T will support all government efforts to protect the integrity of messages in transit where these messages are protected by encryption methods including site-to-site VPN or SSL/TLS VPN services. AT&T will also support the use reconciliation routines such as checksums, hash totals, or record counts to protect the receiver from malicious changes to a message by confirming a transmitted message has not been altered in transit as necessary.
Use of mobile code	<ul style="list-style-type: none"> ■ The system will be configured to prevent downloading mobile code or executable content if there is no requirement to do so. Downloading mobile code and executable content from a controlled interface between interconnected systems will be permitted only when boundary protection devices are appropriately configured and will be approved by the client agency. If mobile code or executable content is obtained via the web, the following will be applied: <ul style="list-style-type: none"> — All mobile code or executable content employed within the system will be approved by the ISSO or, if the system is operating under an agency TO requiring ATO, the agency AO. — A code review and quality control process for deploying mobile or executable content will be implemented and documented.
Documentation	<ul style="list-style-type: none"> ■ Documentation is a security control explaining how software/hardware is to be used and formalizes security and operational procedures specific to the system. System documentation includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to the automated information system security, including backup and contingency plans and descriptions of user and operator procedures. Typical system-related documentation is listed below: <ul style="list-style-type: none"> — A system security plan; — System-specific rules of behavior; — System risk assessment report; — Vendor-supplied documentation of purchased hardware and software; — Network diagrams and documentation on setups/configuration of routers and switches; — Justifications and management approval to use copyrighted software, shareware, or any personally owned software or equipment; — Application documentation for any in-house applications; — Software and hardware testing procedures and results; — Standard operating procedures for equipment and system interfaces; — User manuals; — Emergency procedures; — Configuration management plans; — Emergency change procedures such as procedures for emergency changes to system software; — Log of distribution and implementation of new or revised software; — The system contingency plan, including backup procedures; and — Written agreements regarding how data is shared between interconnected systems.

Control Requirement	Description
Security awareness and education	<ul style="list-style-type: none"> Security awareness is communicated to government users via Service Introduction Packets and Best Practices information brochures. The EIS subscriber website will include information about EIS security policies, practices, and procedures. AT&T vendors are contractually obligated to comply with company policy as well as government requirements in support of the EIS contract. AT&T EIS security manager ensures that the appropriate vendor and contractor personnel are trained on the security policies and procedures as required. AT&T personnel who perform specific security roles, such as system administrator, security administrator, and database administrator, will undergo additional specialized training focused on their respective role. In addition, all personnel with physical and/or logical access to a client agency's system will (1) receive the system rules of behavior, a copy of which will be signed and returned to the designated custodian, and (2) have access to applicable client agency security procedures and policies.
Incident response capability	<ul style="list-style-type: none"> A formal incident response capability will be available and exercised at least annually. The capability and supporting procedures will be documented. The capability will include the following: <ul style="list-style-type: none"> Security incident monitoring and tracking procedures, including (1) how to recognize and handle security incidents and (2) procedures for revising the incident handling procedures after an incident occurs. System performance monitoring procedures to be used to analyze network performance logs in real time to look for availability problems, including active attacks. Reporting to the appropriate emergency response. Receiving and responding to alerts and advisories. A process will be developed to identify the sources of alerts and advisories to be monitored, the personnel responsible for monitoring and responding to alerts and advisories, and response guidance. Designating the individual(s) responsible for testing and maintaining the incident response capability.

- Technical Controls:** Technical controls are those executed by the computer system. Technical controls must be implemented to provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls always requires significant operational considerations and must be consistent with the management of security within the organization. **Table A-2.2-2** describes the types of control topics associated with operational controls. (NIST SP 800-37, Section 3.3, *RMF Step 3 – Implement Security Controls*)

Table A-2.2-2. Technical Control Topics. *Technical controls consist of the following requirements.*

Control Requirement	Description
Identification and authentication	<ul style="list-style-type: none"> This section represents a scenario that typifies the Identification and Authentication section of an AT&T security plan. Off-the-shelf solutions will not be used for task orders under EIS, but will be customized to reflect the requirements of a specific system in a specific agency. The first step is to determine the method of authentication and develop procedures and policies to enforce this method. For instance, if passwords are used, then the procedures and policies would be as follows: <ul style="list-style-type: none"> The System Administrator issues the initial password; The initial password expires at the time of its first use and the password owner must supply a new password;

Control Requirement	Description
	<ul style="list-style-type: none"> — Passwords cannot be the same as the user ID and must have at least three of the following: English uppercase, English lowercase, numerics, and special characters; — Minimum length of eight characters permitted; — Passwords expire every 90 days (enforced by the system); — Expired passwords disallowed after 6 generations; — User accounts disabled after no more than three consecutive invalid attempts (must be reinstated by an administrator); — Vendor-provided default passwords disabled or changed; — No shared accounts, including guest and training accounts, are defined; — No clear text display of passwords allowed on the screen; — Passwords stored as a hash or with one-way encryption; — System administrator passwords transmitted and stored with one-way encryption to prevent anyone from reading the clear-text version; — Passwords, IDs, or application user codes must not be entered in a file or record maintained in the system for the purpose of logging on automatically. ■ Depending on the system sensitivity, the agency's requirements for strong authentication and other factors, the customized security plan may specify stronger authentication tools, methods, and procedures (such as the use of one-time passwords).
Logical access control	<ul style="list-style-type: none"> ■ Logical access controls are the protection mechanisms that limit user's access to information and restrict their forms of system access to what is appropriate for them. These controls include policies that determine a user's level of system access, the procedures by which users are authorized appropriate access, the requirements for monitoring and maintaining access controls, and the system's technical features that enforce logical access controls.
User authorization	<ul style="list-style-type: none"> ■ Each user's access to an EIS system contracted to AT&T will be restricted to the fewest privileges that the user needs to perform their assigned duties. Where practical, critical functions will be divided among different individuals. When not practical, any variations from this requirement will be documented. There will be no shared administrative user accounts. Each privileged user has a personal account, so that all administrative activities are auditable. ■ There will be a formal process for requesting, establishing, issuing, and closing user accounts. An access control form will be developed to document access requests, justifications, and approvals. Compliance with requirements for least privilege, separation of duties, and unique accounts will be fully documented as part of the justification provided on the access control form. ■ A government-designated individual must approve access privileges. The access control process requires this individual review the Access Control Lists not less than twice yearly to ensure that accesses are current and appropriate. All inactive accounts must be deleted to prevent unauthorized access and permissions must be changed to reflect any changes in a user's assigned duties.
Protection from unauthorized access	<ul style="list-style-type: none"> ■ For EIS systems and/or networks with firewall and/or IDS protection customized for that particular system or network, AT&T will describe the related measures to help protect the system in a secure enclave. ■ AT&T will identify any firewalls, IDS, and other devices installed to protect the system/network's perimeter. We will also describe the configuration of those devices. Generally, firewalls are to be configured to exclude any traffic except that which is specifically allowed. Any exceptions will be justified and documented. The IDS is to be configured to monitor site traffic for potential misuse or policy violations and recognize patterns of misuse, such as suspicious or unauthorized activity. ■ Other controls to protect EIS systems from unauthorized access include secure configuration of system devices by removing access to unneeded and unnecessary services from operating systems. Such unneeded or unnecessary services might include file transfer protocol (FTP), Telnet, compilers, and software development tools, if they are deemed to present security vulnerabilities in a specific situation.

Control Requirement	Description
Public access controls	<ul style="list-style-type: none"> ■ If a client agency's EIS system task order provides for public access, AT&T will address the additional security controls needed to protect the integrity of the system and the confidence of the public in the system. Such controls include segregating information made directly accessible to the public from official agency records. Other controls AT&T has designed into federal government public-facing web sites include the following: <ul style="list-style-type: none"> — Some form of user identification and authentication; — Digital signatures to enhance authentication; — Access control to limit what the user can read, write, modify, or delete; — Controls to prevent public users from modifying information on the system; — CD-ROM for on-line storage of information for distribution; — Verify programs and information distributed to the public are virus-free; and — Audit trails.
Warning banner	<ul style="list-style-type: none"> ■ The Computer Fraud and Abuse Act of 1986 (Public Law 99-474) requires that a warning message be displayed notifying unauthorized users they have accessed a U.S. government computer system and unauthorized use can be punished by fines or imprisonment. Although some federal government systems, such as FirstGov.gov, are intended for unrestricted use by the general public (a situation not prevalent when Public Law 99-474 was enacted), all systems that input, process, or store government information must comply with the law. ■ Therefore, for all access to a government system, with the exception of public requests for site content which will include the warning message cited in Section III.8, an approved agency warning banner will be displayed on all servers prior to user access, as required by NIST guidelines.
Audit trails	<ul style="list-style-type: none"> ■ To increase individual accountability, each user must have their own account, with a unique login ID and password (accounts must not be shared), and all privileged user activities will be logged so audit data will be available for review. Where possible, necessary administrator access must be granted through user accounts rather than through root access. ■ Since each user's security-related activities will be subject to recording and routine review for inappropriate activities, audit trails must be of sufficient detail to facilitate reconstructing events if compromise or malfunction occurs or is suspected. ■ AT&T defines that all resources to which access is controlled including applications and operating systems have the capability of generating security audit logs. All security logging mechanisms must be active from the first system initialization. These mechanisms include any automatic routines necessary to maintain the activity records and cleanup programs to ensure the integrity of the security audit/logging systems. ■ The audit logs will be secured. Access to online audit logs will be strictly controlled, preferably through separation of duties between system administrators who administer the access control function, for example, and those who administer the audit trail. AT&T will identify the individual(s) responsible for reviewing security activity logs and the frequency of their reviews. ■ Furthermore, the individuals responsible for information security will review the audit trail following a known system software problem, a known violation of existing requirements by a user, or any unexplained system or user problem. The individual(s) responsible for these audit-related tasks will be identified for each client agency task order. ■ Backup mechanisms and procedures exist to transport audit logs off the system prior to these logs being purged.

A-2.3 Implementation of Security Controls [C.1.8.7]

We review our systems thoroughly against security controls, such as those found in NIST SP 800-53, to determine which of those controls need to be implemented. This includes the allocation of security controls, as discussed previously in **Section A-2.2**, into system-specific, common and hybrid controls. Additionally, while assembling a

system's authorization package, the AT&T Information System Security Officer (ISSO) determines which controls apply to the related technology, based on how the system and sub-systems are implemented. In some cases, certain security controls will require additional components or technologies to be deployed. Additionally, some security controls may need to reference already implemented sub-systems of other controls, and in some cases, certain security controls are not applicable based on how the system is designed and deployed.

A-2.4 Assessment of Security Control Effectiveness [C.1.8.7]

The effectiveness of the security controls against a deployed system can be determined by objectives for security control assessment within the security assessment plan (SAP). The SAP describes what technologies and sub-systems are to be assessed and from this, the actual assessment will determine if there are any vulnerabilities or weaknesses of a system's technologies or sub-systems against the applicable security controls.

Based on the number and types of vulnerabilities, an assessor builds a risk posture for the system. An AO or designated representative analyzes the risk posture to determine the effectiveness of the security controls for a given system. From that analysis, the AO or designated representative decides whether or not to grant the system the authority to operate.

A-2.5 Authorization of the Information System [C.1.8.7]

The authorization of an information system depends on several factors:

- Security authorization package;
- Plan of Actions and Milestones (POA&M);
- Risk determination of the system security platform; and
- Risk acceptance of the system security platform.

Security Authorization Package: Our approach to assembling a security authorization package rests on the guidance in NIST Special Publication (SP) 800-53, Rev. 4, and GSA IT Security Procedural Guide 06-30, *Managing Enterprise Risk*. The process and deliverables consist of the following:

1. Categorize the system and document the results of the security categorization in the system security plan (SSP);

2. Describe the system, including system boundary, in the SSP
3. Register the system with appropriate organizational program/management offices
4. Identify the common controls and document them in the SSP
5. Select the system security controls and document them in the SSP
6. Develop a continuous monitoring strategy for monitoring security control effectiveness and any proposed/actual changes to the system and its environment of operation
7. Submit the system SSP to the AO for review and approval;
8. Implement the security controls specified in the SSP;
9. Document the security control implementation, as appropriate, in the SSP providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs);
10. Develop a Security Assessment Plan (SAP) and submit to the AO or their designee for review and approval;
11. Assess the system security controls in accordance with the SAP;
12. Prepare the security assessment report (SAR) to document any issues, findings, and recommendations from the security control assessment;
13. Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate;
14. Prepare a plan of action and milestones (POA&M) based on the SAR findings and recommendations, excluding any remediation actions taken; and
15. Assemble the security authorization package and submit it to the AO for authorization.

The basic authorization package consists of the following deliverables:

- SSP;
- SAR; and
- POA&M.

The authorization package also includes additional documentation as follows:

- Any applicable Interconnection Security Agreements (ISAs);
- Control Tailoring Workbook;

- System Design Document (SDD);
- NIST SP 800-53, Rev. 4, Control Summary Table;
- Rules of Behavior (RoB);
- System Inventory;
- Contingency Plan (CP), Disaster Recovery Plan (DRP), and Business Impact Assessment (BIA);
- Contingency Plan Test Plan (CPTP);
- Privacy Impact Assessment (PIA);
- Configuration Management Plan (CMP) with System Baseline Configuration and EIS2020 information systems configuration settings;
- Incident Response Plan (IRP);
- Incident Response Test Report (IRTR);
- Continuous Monitoring Plan (CMP);
- Vulnerability scan outputs, as appropriate; and
- Code Review Report, as appropriate.

POA&M: AT&T develops and maintains a system POA&M as directed by the GSA IT Security Procedural Guide 06-30, *Plan of Action and Milestones* (POA&M), and manages vulnerability scanning findings and reports them with the POA&M, on either a monthly or quarterly basis, as required by the authorizing government program office. This enables us to implement a compliant, orderly, approval process that yields risk and vulnerability statuses on an ongoing basis.

We will develop a POA&M to document planned remedial actions to correct weaknesses or deficiencies from security assessments and continuous monitoring activities, including vulnerability scans. The POA&M captures the following elements:

- Weaknesses/vulnerabilities;
- Milestone changes;
- Point of contact for remediation;
- Source that identified the
- Additional resources needed to support weakness/vulnerability; and
- remediation efforts;
- Status.
- Scheduled completion date;

The AT&T system ISSO will format the POA&M, based on a template provided by the appropriate government organizational program/management office. To maintain

accuracy and to meet the government's periodic reporting requirements the POA&M will be updated either monthly or quarterly as required.

The system ISSO updates and delivers the POA&M in the specified timeframe, based on the findings of the security control assessments and ongoing monitoring activities including vulnerability scanning. We will include, in the quarterly POA&M submission, an action step to remediate high and medium items from scans. The scan reports contain details on any issues noted. The scan reports are available to the government as part of the quarterly POA&M submission.

Risk Determination of the Security Platform: The determination of risk of a system or security platform is based on:

1. **Vulnerability**, i.e., what is the severity of the risk;
2. **Impact**, i.e., what would it mean to us if the vulnerability were exploited; and
3. **Threat**, i.e., what is the likelihood of such an exploitation.

After assessing each of the three risk factors and assigning them individual categories of: High, Medium or Low, they are then combined to obtain the overall risk assessment category:

1. High
2. Medium
3. Low

Risk Acceptance of the Security Platform: Either a panel or individuals within a government organizational program/management office will review the system security authorization package for security risk. Based on their review and recommendations of the authorization package, the government organizational program/management office AO determines the level of risk that the system represents and whether the risk is acceptable. If the AO finds the risk level to be acceptable, then the official issues the Authorization to Operate (ATO).

A-2.6 Ongoing Monitoring of Security Controls and the Security State of the Information System [C.1.8.7]

Ongoing monitoring of security controls and security state of the information system consists of the following:

- Continuous monitoring of the system;
- Logical maintenance of the system components; and
- Assessment of potential security impacts.

Continuous Monitoring: Post authorization of a system, the AT&T ISSO assembles a continuous monitoring report either every month or quarterly, based on the authorizing government program office requirements for continuous monitoring. The report includes a POA&M, as discussed previously in **Section A-2.5**, which records any vulnerabilities in the system. Those vulnerabilities are assigned a risk level of high, medium or low. Additionally, based on the types of vulnerabilities, the ISSO may assemble a plan of action to mitigate any vulnerabilities that appear to be patterns over time or for vulnerabilities that affect common system technologies or infrastructure.

Logical Maintenance: Our Information Technology Office (ITO) is charged with monitoring and maintaining the EIS systems to ensure those systems have the latest hardware deployed or software patches updated. The ISSO will alert ITO of hardware update or patch update requirements per the associated vulnerabilities in the POA&M. It is then up to ITO to test and implement any updates to mitigate those vulnerabilities. At no time during this process will AT&T publish or disclose the details of hardware or patch updates, or any safeguards designed or developed under a TO or otherwise provided by the Government, without written consent by the CO.

Assessment of Potential Security Impacts: Relative to the POA&M, the ISSO and ITO will monitor the types of vulnerabilities that impact the information system and determine if there may be potential for future security impacts. The vulnerabilities will be vetted to determine any potential threats to the information system and if any physical or logical changes to the system boundary are warranted.

If changes need to be made to the information system, the ISSO will request those changes from the system owner. When the changes are made by the system owner, the ISSO will then update the security authorization documentation, including the SSP, as to the proposed changes made or to be made to the information system. The ISSO will also alert the authorizing officer or designated representative of any changes made to the security authorization documentation for purposes of review and risk assessment.



General Services Administration (GSA)

Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

GS00Q17NSD3000

Appendix B — MTIPS Risk Management Framework Plan

APPENDIX B — MTIPS RISK MANAGEMENT FRAMEWORK PLAN

[L.29(3)(B); L.29.2.2; L.11; C.1.8.7; C.1.8.7.1; C.2.8.4.5; C.2.8.4.5.5]

Ensurance of Delivery of System Security for MTIPS [L.29.2.2; C.1.8.7; C.2.8.4.5]

RFP Section L.29(3)(b) states that an MTIPS Risk Management Framework Plan shall be submitted as identified in RFP Section C.2.8.4.5, if MTIPS is offered. Further, the RFP Section C.2.8.4.5 points to the requirement in RFP Section C.2.8.4.5.4 which obligates offerors to deliver a System Security Plan (SSP). This appendix is provided per the requirement in the RFP Section C.2.8.4.5.2 that states, "The contractor shall submit a Risk Management Framework Plan describing its approach for MTIPS security compliance. This plan shall be submitted with the proposal in accordance with NIST SP 800-37." The SSP will be delivered initially within 30 days of the NTP as identified in RFP Section F.

To assist GSA in protecting the confidentiality of Government information and to maintain the availability of the system, AT&T MTIPS is implemented and operated in accordance with a comprehensive Risk Management Framework (RMF). This approach to risk management is consistent with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*. Our RMF is a risk-based approach to provide security for MTIPS under this contract, and complies with the applicable IT security directives, standards, and policies, such as listed in RFP Section C.2.8.4.5.1.

AT&T applies the approach that risk is a measure of the extent to which an entity is threatened by a potential circumstance or event and a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of the occurrence of the event.

To manage and reduce risk to the lowest practical level, the AT&T MTIPS RMF plan follows the six-step NIST RMF approach that includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The AT&T MTIPS RMF plan follows the entire life cycle of a delivered service, beginning in the development phase through continuous monitoring and service decommissioning and

removal of Government information. The AT&T MTIPS RMF plan outlines the processes that are followed to implement changes to MTIPS should GSA choose to allow changes in the service security profile initiated either by an agency with GSA prior approval or due to GSA approved lifecycle updates in technology or due to evolving security requirements. In addition:

- AT&T will confirm, where appropriate, the implementation of the requirements identified in the FAR (see Section I, 52.224-1, “Privacy Act Notification” and FAR 52.224-2, “Privacy Act.”)
- AT&T will cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the federal government’s agent.
- AT&T will afford the government logical and physical access to the contractor’s facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request.

B-1 The AT&T MTIPS Risk Management Framework Plan [C.2.8.4.5.2; C.2.8.4.5.5]

The AT&T MTIPS RMF plan provides the following:

- Promotes the concept of near real-time risk management through the implementation of robust continuous monitoring processes supporting ongoing authorization as applicable
- Applies automation to provide system operations teams and AT&T senior leaders with the necessary information to make risk-based decisions on system operations
- Integrates information security into the MTIPS architecture and system development life cycle
- Establishes responsibility and accountability for security controls implemented in AT&T MTIPS infrastructure and inherited by MTIPS, such as common controls across shared management infrastructure
- Provides the methodology and guidance to integrate required security controls into the AT&T MTIPS architecture and system development life cycle processes, providing the Government with MTIPS service
- Provides comprehensive protections against threats to Confidentiality, Integrity or Availability.

As shown in **Figure B-1-1**, the RMF overlays the standard system development life cycle phases — Initiate, Design, Implement, Operations & Maintenance, and Dispose. We implement, assess, and monitor ongoing compliance with the applicable baseline security requirements specified in NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for moderate- impact systems and other related GSA

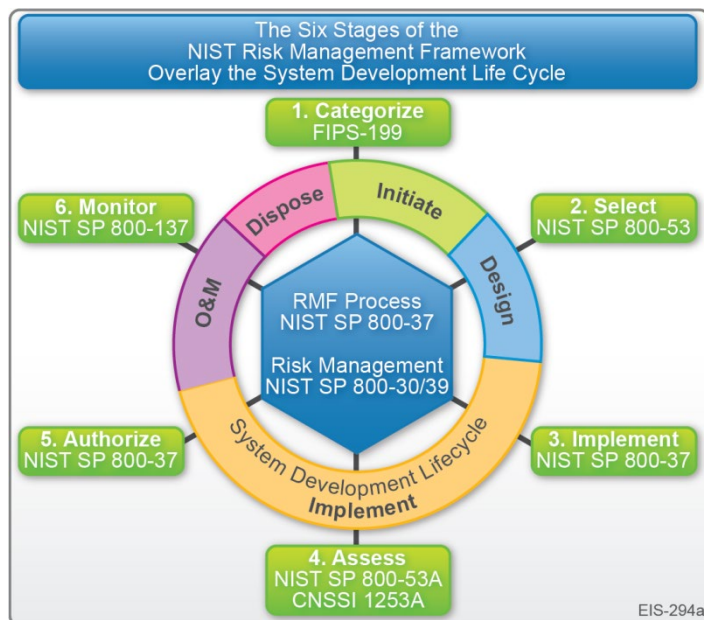


Figure B-1-1. AT&T RMF Life Cycle. Properly implemented, the RMF synchronizes information security with system development and maintenance, resulting in more thorough and economical compliance throughout the life cycle.

directives and guides. Our MTIPS RMF approach is based on the guidance in NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* and GSA IT Security Procedural Guide 06-30, *Managing Enterprise Risk*. The processes and deliverables of the AT&T MTIPS RMF Plan consist of the following:

- Follows the GSA or agency Task Order (TO) for system impact categorization and documents the security categorization in the Service System Security Plan (SSP). (NIST SP 800-37, Section 3.1, *RMF Step 1 — Categorize Information System*)
- Describes the MTIPS service infrastructure in the SSP, including system boundary as defined in NIST SP 800-37, Section 2.3, *Information System Boundaries*.
- Registers the systems that support MTIPS with appropriate AT&T organizational program/management offices for oversight and system owner identification.
- Identifies any common controls that are inherited from systems outside the MTIPS infrastructure system boundary and document them in the SSP. (NIST SP 800-37, Section 2.4, *Security Control Allocation*)
- Verifies the security controls from the NIST 800-53, Rev. 4, baseline for a high-impact system and any additional controls required by GSA and/or agency provided TO

needed to address specific information security risks and document them in the SSP (NIST SP 800-37, Section 3.2, *RMF Step 2 — Select Security Controls*) [Section C.2.8.4.5.2]

- Develops a continuous monitoring strategy for monitoring security control effectiveness and any proposed/actual changes to the service infrastructure and its operating environment. The AT&T continuous monitoring strategy reflects, and is consistent with, the NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* and the GSA organizational continuous monitoring strategy and program as described in GSA IT Security Procedural Guide: Information Security Continuous Monitoring Strategy, CIO-IT Security-12-66. (NIST SP 800-37, Section 3.2, *RMF Step 2 — Select Security Controls/Monitoring Strategy*)
- Implements the security controls specified in the SSP. (NIST SP 800-37, Section 3.3, *RMF Step 3 — Implement Security Controls*)
- If required by an agency TO, submits an agency specific MTIPS SSP and other required documentation and artifacts of system that demonstrate adherence to the required NIST, GSA, and agency-specific security controls to the agency's Authorizing Official (AO) for review and approval.
- Documents the security controls implementation in the SSP, providing a functional description of how each control is or will be implemented, including planned inputs, expected behavior, and expected outputs. (NIST SP 800-37, Section 3.3, *RMF Step 3 — Implement Security Controls/Security Control Documentation*)
- Develops a Security Assessment Plan (SAP) for testing the service infrastructure to verify that the required controls specified in the approved SSP are implemented as described and providing the appropriate level of risk management. The SAP describes what technologies and sub-systems are to be assessed and from this the actual assessment will determine if there are any vulnerabilities or weaknesses of a system's technologies or sub-systems when tested against the applicable security controls. For an agency specific MTIPS solution that is required to operate under an authorization specified in a TO, we will submit the SAP to the AO or their designee for review and

approval. (NIST SP 800-37, Section 3.4, *RMF Step 4 — Assess Security Controls/Assessment Preparation*)

- Executes the SAP to assess the effectiveness of service infrastructure security controls. The AT&T program Information Systems Security Officer (ISSO) or for systems required to operate under a TO specified authorization, an agency AO or designated representative analyzes the SAP testing results to determine the effectiveness of the security controls for MTIPS. From that analysis, the ISSO, agency AO, or designated representative decides whether or not to grant the system the authority to operate. (NIST SP 800-37, Section 3.4, *RMF Step 4 — Assess Security Controls/Security Control Assessment*)

Where applicable for service infrastructure that has an agency TO authorization requirement, the AT&T MTIPS RMF outlines how AT&T works with an independent third party assessor. The assessor can be either contracted by AT&T or an agency designee to perform the required testing of the service infrastructure security controls.

- Prepares a Security Assessment Report (SAR) to document any issues, findings, and recommendations from the security control assessment. (NIST SP 800-37, Section 3.4, *RMF Step 4 — Assess Security Controls/Security Control Assessment*)
- Conducts initial remediation actions based on the findings and recommendations in the SAR and reassesses remediated control(s), as appropriate. (NIST SP 800-37, Section 3.4, *RMF Step 4 — Assess Security Controls/Security Control Assessment Remediation*)
- Prepares a Plan of Action and Milestones (POA&M) based on the SAR findings and recommendations, excluding any remediation actions taken. For service infrastructure that is operating under an agency authorization, the Government provides final determination of open finding risk rating (critical/high, moderate, or low). (NIST SP 800-37, Section 3.5, *RMF Step 5 — Authorize Information System Plan of Action and Milestones*)
- For service infrastructure operating under an agency authorization as stated in a TO, the following action is provided per the AT&T MTIPS RMF plan (NIST SP 800-37, Section 3.5, *RMF Step 5 — Authorize Information System Security Authorization Package*):

- Assembles the security authorization package and submits to the AO for authorization, where the level of effort is based on the NIST FIPS Pub 199 categorization of High Impact for MTIPS.

The basic authorization package consists of the following deliverables:

- SSP (in accordance with NIST SP 800-18, Rev 1) with required appendices
- SAR
- POA&M

If the MTIPS infrastructure inherits common controls, then we include either the authorization package for the common controls or a reference to the documentation.

If any inherited common controls are provided by an external provider this information is included in the AO to support the authorization decision.

Also included with the authorization package are SSP appendices and additional documentation as specified in the TO, per NIST and GSA guidelines

[Section C.2.8.4.5.4, (1-15)]:

- Applicable Interconnection Security Agreements (ISAs)
- Control Tailoring Workbook (CTW)
- Rules of Behavior (RoB)
- System Inventory, as a section in the System Design Document (SDD)
- Contingency Plan (CP), including the Disaster Recovery Plan (DRP) and Business Impact Assessment (BIA)
- Contingency Plan Test Plan (CPTP)
- Privacy Impact Assessment (PIA)
- Configuration Management Plan (CMP) with system baseline configuration and BSS configuration settings
- Incident Response Plan (IRP)
- Incident Response Test Report (IRTR)
- Continuous Monitoring Plan (CMP)
- Vulnerability scan outputs, as required
- Code Review Report, as required

As MTIPS is an existing service with an Authorization to Operate (ATO), the system currently operates under RMF Plan, *Step 6, Monitor Security Controls, the Continuous*

Monitoring of Security Controls of the AT&T MTIPS service with a Continuous Monitoring Plan.

The on-going security monitoring activities consist of the following:

- Assesses the security impact of proposed or actual changes to the MTIPS Infrastructure and its operating environment
- Annually assesses a subset of the MTIPS Infrastructure operational policy security controls consistent with the continuous monitoring plan
- Remediates vulnerabilities based on the results of the ongoing monitoring activities and risk assessment, as prescribed and tracked through the POA&M
- Maintains the SSP, SAR, and POA&M
- Prepares and submits system security status reports per the continuous monitoring plan, to AT&T leadership and the agency AO if an agency needs a custom MTIPS service that would require an agency authorization.

The AT&T MTIPS RMF is a comprehensive plan designed to deliver MTIPS with infrastructure that is designed, implemented, operated, and monitored to provide the Government with services that are verified secure and continuously reviewed for strict adherence to GSA and agency security requirements. (NIST SP 800-37, Section 3.6, *RMF Step 6 — Monitor Security Controls*)

B-2 The AT&T MTIPS RMF Plan Management and Oversight **[C.2.8.4.5; C.2.8.4.5.2]**

The AT&T MTIPS RMF plan is managed by the AT&T Information Assurance (IA) organization. The IA organization provides independent oversight of the system and service infrastructure development and operations organizations at AT&T. The IA organization's RMF-defined functions include the following major tasks:

(NIST SP 800-37, Section 1.2, *Purpose and Applicability*)

- Selects the GSA, agency specific, and AT&T security controls that systems and service infrastructure supporting MTIPS follow based on the RMF plan, GSA guidance of risk determination, and/or agency specification. The IA organization provides guidance to all technical, operational, and managerial staff on how each security controls is be implemented.

- Verifies that the technical, operational, and managerial organizations document how the selected controls are implemented and followed. This documentation includes the SSP, SSP appendices, technical system descriptions, personnel suitability verification processes, and other artifacts used as reference to demonstrate adherence to an accepted system risk profile.
- Tests and/or supports an agency's independent assessor to perform preproduction testing of all technical, operational, and managerial security controls verifying compliance prior to providing service to the Government.
- Reviews and verifies that all personnel supporting systems and service infrastructure hold the appropriate credentials and suitability to access restricted Government information.
- Performs system lifecycle continuous monitoring of the technical, operational, and managerial security controls verifying that the system and service infrastructure is operated in accordance with the approved risk profile. This monitoring includes monthly testing and POA&M reporting of technical control implementation, verifying adherence to operational policies, and reviewing managerial oversight per NIST and GSA guidelines. The continuous monitoring performed by the IA organization verifies that the infrastructure is in constant compliance with all required security controls and reports on any identified deficiencies to senior leadership and the GSA AO using the POA&M as the reporting method.
- Works together with the GSA agency AO, where service infrastructure operates under the GSA ATO on required reauthorization deliverables. The AT&T MTIPS RMF plan and the Continuous Monitoring Plan provides support for continuous compliance to allow for continuing authorization should GSA so choose. This is accomplished by providing artifacts quarterly, and during the annual assessment, that demonstrate verification of compliance, reducing the cost of Assessment and Authorization with an assessor over three years.
- Engages in disaster recovery testing, incident response testing, and security events mitigation.

B-2.1 IA Organization Team Alignment in Support of the MTIPS RMF Plan [C.2.8.4.5.2]

The IA organization is a member of the AT&T Compliance and Governance organization in the Services Assurance division. The IA organization is independent of the direct reporting chain from Service Development, Service Operations management, and customer Program Management organizations. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The ISSOs have direct working relationships with all system and service infrastructure owners and attend project meetings to facilitate communications, expectations, system status, change control, patching, planned upgrades, and incident engagement.

Figure B-2.1-1 depicts the AT&T IA Organization. (NIST SP 800-37, Section 2.2, *System Development Life Cycle*)

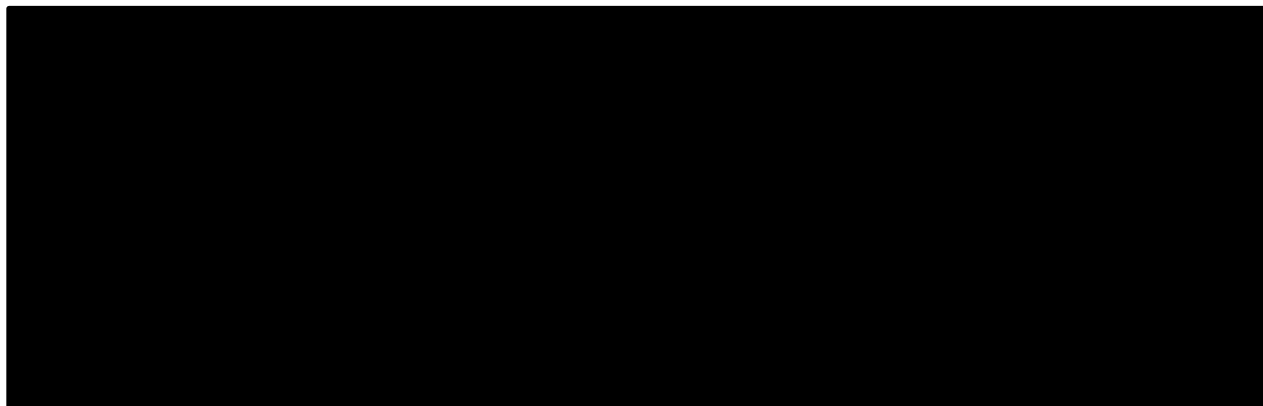


Figure B-2.1-1. AT&T IA Organization. [REDACTED]

B-2.2 IA Organization Team Alignment in Support of the RMF Plan [C.2.8.4.5.4; C.2.8.4.5.5; C.2.8.4.5.5.1]

The IA ISSO assigned to MTIPS has the primary oversight to execute the RMF plan for the system. When developing the infrastructure supporting MTIPS, the ISSO follows applicable NIST and OMB guidance on the selection and implementation of the security controls. The ISSO follows the specific guidance below for providing the implementation

and operation teams on the execution of specific security controls. The AT&T MTIPS RMF plan places the NIST SP 800-53, Rev. 4, controls, GSA and agency specific security controls, and AT&T corporate controls into three logical categories for tracking and management oversight. These categories are management controls, operational controls, and technical controls. Each of these categories are used to identify which AT&T organizations assign a resource to work with the ISSO to implement and verify control implementation compliance.

The implementation of the controls, while broken down into categories of managerial, operational, and technical controls for a specific system to provide clear and direct ownership, also follow the guidance for the types of security controls provided in NIST SP 800-37, Section 2.4, *Security Control Allocation*. AT&T follows the concept of identifying controls as they are implemented across the organization as:

- **System-specific Controls:** controls that provide a security capability for a designated information system
- **Common Controls:** controls that provide a security capability for multiple information systems
- **Hybrid Controls:** controls that have both system-specific and common characteristics
AT&T follows NIST guidance to identify common or inherited controls and the senior management and operational resources responsible to implement and operate the common controls. This is accomplished in accordance to the applicable NIST SP 800-53, Rev. 4, security control guidance and consistence with the risk profile of specific systems that use the common controls. (NIST SP 800-37, Section 3.0, *Executing the Risk Management Framework Tasks*)
- **Management Controls:** Management controls are actions taken to manage a system's development, maintenance, and use. This includes system-specific policies, procedures, assignment of individual roles and responsibilities, and rules of behavior. These controls are the overriding practices that must be followed so the systems operate as expected. (NIST SP 800-37, Section 3.3, *RMF Step 3 — Implement Security Controls*)
- **Operational Controls:** The operational controls address security mechanisms that focus on methods that are primarily implemented by people, as opposed to those

implemented by systems. The methods often require technical or specialized expertise and often rely on management activities as well as technical controls. **Table B-2.2-1** describes the types of control topics associated with operational controls. (NIST SP 800-37, Section 3.3, *RMF Step 3 — Implement Security Controls*)

Table B-2.2-1. Operational Control Topics. *Operational controls consist of the following requirements.*

Control Requirement	Description
Personnel security	<ul style="list-style-type: none"> These controls provide guidance on restricting access to appropriately credentialed and suitable personnel. The controls also provide guidance on applying the concept of Least Privilege to Role Base assignments that restricts access to no more functionality than each person needs to execute their assigned role, as outlined in the NIST guidance. Personnel security also includes log audit controls to trace user activity back to each use. Finally the controls establishes procedures for maintaining the security of the system when personnel who have had access granted no longer require access. The depth, breadth, and rigor of the personnel security controls required for a system vary depending on numerous factors, including the system's sensitivity and, where applicable, the authorizing agency's unique requirements. The following subsections represent a scenario that somewhat typifies the Personnel Security section of an AT&T security plan. It is important to note that the AT&T MTIPS RMF plan is used as a minimum guideline and is a starting process that will be customized for MTIPS for which an agency contracts for support under EIS. Like all other security plan sections, it will be customized to reflect the requirements of MTIPS in a specific agency as required when specified in a TO and if requested changes are approved by GSA.
Personnel security management	<ul style="list-style-type: none"> The AT&T MTIPS RMF Plan provides guidance on the personnel security management baseline to meet GSA requirements for delivering MTIPS that is implemented and operated in accordance with the NIST SP 800-53, Rev. 4 High Impact Baseline security controls operated with personnel who have been granted HSPD-12 suitability at the appropriate Position of Public Trust Level based on their Role, and in accordance with FAR Part 52.204-9. AT&T will designate an individual whose role includes coordinating the aspects of the task order that pertain to obtaining and maintaining security clearances at the appropriate levels for contractor personnel. The individual's responsibilities will include such activities as obtaining and maintaining security clearances, if needed, and suitability, and related coordination with the agency, and monitoring approvals for persons with physical access to sensitive facilities. The AT&T security office has the experience and knowledge to manage any level of required personnel credentials and currently initiates/processes an average of 56 new security credentials per month.
Sensitivity of positions	<ul style="list-style-type: none"> The sensitivity of positions that require system access will depend on the classification level of the system. There are expected to be two classifications of users, 1) privileged administrative users, such as system administrators, and 2) generic users. Work performed under EIS task order(s) may fall within one or more of the risk categories defined below. Therefore, AT&T personnel will undergo background investigations commensurate with the risk factor associated with the duties of each position. <ul style="list-style-type: none"> High Risk positions have the potential for exceptionally serious impact involving duties especially critical to the GSA. These may include computer positions responsible for planning, directing, and implementing the system's security program; directing, planning, and designing the system, including the hardware and software; or accessing the system during its operation or maintenance in a way that would enable them to cause grave damage or realize significant personal gain. Moderate Risk positions are sensitive positions that have the potential for moderate to serious impact involving duties very important to the GSA. These may include computer positions of a lesser degree of risk than seen in High Risk positions, as defined in OMB Circular A-130, Appendix III.

Control Requirement	Description
	<ul style="list-style-type: none"> — Low Risk positions are non-sensitive positions that do not fall into either of the preceding categories and includes those positions with potential for impact involving duties of limited relation to the GSA.
Required background investigations	<ul style="list-style-type: none"> ■ Background investigations will be conducted and favorably adjudicated, as applicable, for AT&T personnel before work commences. Typical minimum pre-appointment investigative requirements are as follows: <ul style="list-style-type: none"> — High Risk positions may require a Limited Background Investigation (LBI), which consists of a personal subject interview, National Agency Check (NAC), credit history check, written inquiries, record searches covering the preceding five years, and personal interviews covering specific areas during the most recent three year period. — Moderate Risk positions may require a National Agency Check and Inquiries (NACI), which consists of written inquiries and record searches covering specific areas of a subject's background during the preceding five years. — Low Risk positions may require a Federal Bureau of Investigation (FBI) Name and Fingerprint check.
Pre-Appointment background investigation waivers	<ul style="list-style-type: none"> ■ AT&T will work with GSA in situations where a MTIPS staffing and support position decision may be unable to wait for an entire background investigation to be completed. In such cases, it is common for a pre-appointment background investigation waiver to be granted by the authorizing agency. The extent of the background investigation needed to qualify for waivers varies by agency, system sensitivity, and position sensitivity. Typical waiver requirements are as follows: <ul style="list-style-type: none"> — High Risk positions may require a successful NCIC check, vouchering of previous two employers, and a favorable review of forms submitted. — Moderate Risk positions may require a favorable NCIC check and a favorable review of forms submitted. — Low Risk positions may require a favorable NCIC check.
Required security forms	<ul style="list-style-type: none"> ■ AT&T employees holding sensitive positions supporting federal agency systems, requiring HSPD-12 compliance, will complete the following forms [C.2.8.4.5.5.1]: <ul style="list-style-type: none"> — Applicant Fingerprint Card (FD-258) – two sets per applicant; and — Questionnaire for Non-Sensitive Positions (SF-85), or Questionnaire for Public Trust Positions (SF-85 P). ■ AT&T currently has over 3,000 cleared personnel. All AT&T IA personnel have been granted Secret clearances as a minimum; many possess Top Secret clearances; and several have higher levels.
Operational access controls	<ul style="list-style-type: none"> ■ Access to an MTIPS system will be granted based upon the individual's assigned responsibilities with each user restricted to the minimum level of access necessary to perform their assigned duties. When possible, assignments to support critical functions will follow the principal separation of duty and will be divided among different individuals. If impractical, variations from this requirement will be justified and documented. This division or separation of duties will be established and maintained through access controls. Whenever possible, administrator access shall be granted through user accounts rather than through root access. ■ Assignment of user privileges will follow the GSA protocols for requesting, establishing, issuing, and closing user accounts. With ISSO oversight, the AT&T project manager or designee will provide oversight for access requests and approvals. AT&T will develop standard access control documentation that will be used to document access requests, justifications, and approvals for all systems. In addition, AT&T personnel assigned to an EIS task order will comply with the client agency's security policies and procedures, sign the rules of behavior, and follow the procedures developed for the operation and maintenance of the MTIPS system.
Holding users responsible for their actions	<ul style="list-style-type: none"> ■ Two mechanisms will be in place for holding users responsible for their system-related actions: <ul style="list-style-type: none"> — A Rules of Behavior (ROB) document is created specifically for MTIPS . The ROB is issued to all parties with physical and/or logical access to the network. Each person will sign a copy of the rules to acknowledge receipt and the project manager or designee will maintain the signed documents.

Control Requirement	Description
	<p>— The security audit capability and processes described below under Audit Trails will be implemented and maintained. Each system user will have their own account with a unique login ID and password. All security-related user activities will be logged. Each user will have a unique account creating an audit trail of each user's activities. As discussed in the Audit Trails section designated personnel will be responsible for periodically reviewing the administrator activity logs to identify any suspicious activity.</p>
Friendly and unfriendly termination procedures	<ul style="list-style-type: none"> ■ Upon termination or transfer of personnel from duties related to the contracted system environment, regardless if friendly or unfriendly, the ISSO has oversight for the process that requires the AT&T project manager or designee to request and verify that system access has been terminated. ■ Judgment will be exercised in deciding upon the timing of terminating access. In the case of unfriendly terminations, system access will be terminated immediately. If an employee is to be fired, system access will be removed just before or at the same time the employee is notified of dismissal. When an employee gives notice of resignation and is suspected that it may be on unfriendly terms, system access will be terminated immediately. ■ As part of the AT&T employee's exit interview, or at an earlier time if appropriate, the departing employee will be briefed on their responsibilities for confidentiality and privacy with respect to EIS task orders or service infrastructure for MTIPS. Explicit direction will be given relative to what information, if any, is allowed to be disclosed. ■ At the employee's exit interview, or at an earlier time, all tangible access tools, such as authentication tokens and key cards for facility doors, will be retrieved and accounted for. In the case of an unfriendly termination, cipher lock combinations will be changed, and keyed locks will be re-keyed upon the employee's departure.
Physical and environmental protection	<p>— The AT&T MTIPS RMF plan will provide the following controls for each physical site where system devices, media, or other resources are housed in accordance with the corresponding NIST guidelines:</p> <ul style="list-style-type: none"> — Site plans detailing responses to emergencies for IT facilities. — Annual reviews of physical security measures. — Controlled physical access through the use of guards, identification badges, or entry devices such as key cards or biometrics. — Keys or other access devices required to enter these sites, including data center(s), computer room(s), and tape/media libraries. — Properly-secured keys or other entry devices that are not issued. — Cipher lock entry codes will be changed periodically. Frequency will be defined in the SSP for each system where cipher locks are used. — The schedule and off-schedule times at which codes are changed and the individual(s) responsible for ensuring that codes are changed as specified. — Authentication of visitors, contractors, and maintenance personnel who may access these sites. Authentication is done through the use of preplanned appointments and identification checks. — A procedure for signing in and escorting site visitors. A register is maintained that includes the names of the visitor and the person authorizing the visit, visitor's signature, date, and time-in and time-out. — Emergency exit and re-entry procedures to ensure only authorized personnel can re-enter after fire drills and any other similar mass departure/re-entry of the site. — System cabling and other communications equipment closets are physically secured to prevent unauthorized access. — Physical access to routers, switches, telephony gateways, routers, and other sensitive equipment is restricted to authorized personnel. — All perimeter walls and firewalls extend from the structural floor to the structural ceiling. — Interior and exterior windows do not open into a non-secured area. — Environmental protection for IT systems. The means of providing the protection will be documented. — Appropriate fire suppression and prevention devices are installed and properly functioning.

Control Requirement	Description
	<ul style="list-style-type: none"> — Reviews for fire ignition sources such as; failures of electronic devices or wiring, improperly stored materials, and the possibility of arson are performed in accordance with each AT&T operations facility and documented fire code procedures. — Cables leaving and entering the site installed with fire stops. — The temperature and humidity within the facility monitored and controlled to provide an operational environment that conforms to the manufacturer's specifications. — Heating and air-conditioning systems are maintained regularly. — Redundant air-cooling system for the site(s) are provided. — Building plumbing lines are identified and documented. — Reviews of electric power distribution, heating plants, water, sewage, and other utilities are conducted. — Power circuits are clearly identified, dedicated, and meet equipment manufacturer's amperage requirements. — Equipment that is grounded with American Wire Gauge (AWG) #6, meets manufacturer's specifications, and complies with local electrical code. — Uninterruptible power supply(s) (UPS) or backup generator(s) are available to support the system in the event of AC power failure. The UPS or generator(s) will provide a minimum of one hour of power. — Equipment cabinet doors that remain locked. — Controls to mitigate effects of disasters such as floods and earthquakes. — Network administration terminals equipped with the following safeguards: physically located to minimize unauthorized access or viewing; password control and password aging features invoked; timed auto logoff enabled, and protection from unauthorized use. — A risk analysis that considers additional environmental and physical controls for facilities that support large-scale IT operations, such as telecommunication facilities.
Production input/output controls	<ul style="list-style-type: none"> ■ The production input/output controls maintain the security posture of a system's live processing environment and appropriately distribute its data. These controls include help desk and other user support and are used for marking, handling, processing, storage, and disposal of input and output information and media. These controls are also used for labeling and distribution procedures for the input and output information and media. These controls include the mechanisms used to monitor installation and updates to the production environment.
Marking and storing devices and media	<ul style="list-style-type: none"> ■ AT&T protects system devices and electronic media by marking them in accordance with the system's sensitivity to the highest classification level authorized (e.g., Limited Official Use). System devices contain external classification markings authorizing the level of information that can be processed. Data is not stored on electronic media that cannot be adequately secured against unauthorized access. ■ AT&T labels all SSP deliverables as "CONTROLLED UNCLASSIFIED (1)INFORMATION" (CUI) or an AT&T selected designation per document sensitivity. External transmission/dissemination of CUI data to or from a GSA computer will be encrypted using certified encryption modules in accordance with FIPS PUB 140-2, <i>Security requirements for Cryptographic Modules</i>. [C.2.8.4.5.5]
Device and media disposal	<ul style="list-style-type: none"> ■ System devices that have processed, stored, or transmitted sensitive information will not be released from system control until the equipment is sanitized and all stored information has been cleared. For sensitive information, the sanitization method will be approved by the client agency and documented in the customized security plan. If any system IT equipment is maintained under warranty contracts, the contracts will include stipulations that equipment removed from its hosting site will be sanitized before its removal. ■ When no longer required for system support, IT storage media to be re-utilized for unrelated system purposes will be overwritten with software and protected consistent with the data sensitivity and/or at the highest classification level at which they were previously used. If the system processes, stores, or transmits classified data, then classified media will be disposed of in accordance with measures established by the National Security Agency (NSA) and the required disposal procedures of the client agency. ■ Official electronic records will be properly disposed of and if appropriate archived. AT&T will identify any official electronic records related to the system and the approved disposal/archive procedures to be followed.

Control Requirement	Description
	<ul style="list-style-type: none"> The EIS MTIPS Security Manager or designee will maintain records regarding all aspects of the implementation of disposal actions and verify the device or media was sanitized in accordance with NIST guidelines.
Monitor the production environment	<ul style="list-style-type: none"> Production, input/output controls include the mechanisms used to monitor installation and updates to the production environment. A System Test & Evaluation (ST&E) will be developed and executed, either by AT&T or by the agency's designated assessor for systems operated under an authorization as specified in the TO. The ST&E will validate that security requirements for contracted systems and service infrastructure for EIS services are satisfied. The ST&E will test controls as prescribed as well as compliance with secure operating system configuration requirements tested using one or more automated security scanning tools. As part of the ST&E the system will be reviewed to identify and eliminate unnecessary services, ports, and protocols. This review will occur on an annual basis or within six months after there is a significant change to the environment that alters the in-place assessed risk. The system will be reviewed annually or within six months after there is a significant change to the environment that alters the in-place assessed risk for known vulnerabilities and software patches will be installed. AT&T will specify the process by which the system will be reviewed including schedule, tools, methods, and responsible personnel. AT&T will also specify procedures for identifying, downloading, testing, and applying patches, service packs, and hot-fixes. The AT&T MTIPS RMF plan requires that the use of any copyrighted software will be documented. Shareware and personally-owned software/equipment will require a waiver and will be documented. AT&T will include procedures under which any copyrighted software will be used in compliance with applicable copyright laws and will be incorporated into the system's life cycle management process. Other system configuration requirements are as follows: <ul style="list-style-type: none"> Laptops and mobile computing devices (including personal digital assistants [PDAs]) approved for processing sensitive information will not be connected to networks or systems unless the network or system is designed for that functionality. The devices will employ virus protection software and encryption technology. Automatically forwarding e-mail regardless of the forwarding method employed either to the system or through the system if it is a network, is forbidden unless the ISSO or the GSA MTIPS AO grants a waiver.
Contingency planning	<ul style="list-style-type: none"> Critical MTIPS configurations, government sensitive data, and information generated and stored at AT&T MTIPS facilities will have a NIST compliant contingency plan in place throughout the length of the EIS contract period to facilitate continuity of system functions in the event of disruption in computer operations. These contingency plans, also referred to as disaster recovery plans or business recovery plans, will include steps to be taken to ensure preparedness including near real-time mirrored back-up of all servers at off-site locations and plans for timely response after a disruption. This process will be applied to systems that support critical MTIPS services and databases.
Continuity of operations plans	<ul style="list-style-type: none"> Three essential contingency planning activities will be combined to provide for plan related testing, training, and management approval. The plan will be tested and revised as necessary based on the testing. The plan will be tested using the tabletop approach. Using this approach, all personnel expected to implement any part of the plan will be assembled. Using a facilitated workshop methodology the assembled personnel will walk through multiple contingency scenarios validating the steps described in the plan. While the plan may require revision based on the testing, the individuals responsible for executing the plan will have been trained in their responsibilities by participating in the testing scenarios. Additionally, the approval of the key affected parties will be gained through the process. After revisal and approval from the system ISSO, the plan will be distributed to the personnel responsible for executing the plan. Once implemented, the plan will be tested annually or within six months after a significant change to the environment that alters the in-place assessed risk of the affected system.

Control Requirement	Description
Backup and off-site storage	<ul style="list-style-type: none"> Day-to-day security operations and administration will include performing regularly scheduled software backups and managing backup media. Recent software and data backups will be essential if disaster recovery is required regardless if it is natural or intentional. Duplicate backup media is stored off site, in accordance with NIST guidelines, to minimize the risk of being damaged or destroyed with the production environment.
Hardware and system software maintenance and repair	<ul style="list-style-type: none"> AT&T will develop on-site and off-site maintenance procedures. The procedures will include restrictions on who may perform maintenance and repair activities, guidelines and procedures for escorting maintenance personnel who need to work in restricted areas, and guidelines and procedures for securing devices or removable media that must be removed from the site. The capabilities to add, change, or remove system devices, dial-up connections, and network addresses and protocols or to remove or alter programs will be restricted to authorized personnel, as described in the Personnel Security and Logical Access Controls sections.
Hardware and system software configuration management	<ul style="list-style-type: none"> A configuration management process will be in place and documented to maintain control of system changes and to provide a current history of system change. AT&T will prepare a system configuration management plan. The plan will identify the personnel responsible for system configuration management as well as the guidance and procedures for configuration management. In accordance with NIST guidelines, AT&T will address the following requirements: <ul style="list-style-type: none"> Software change request forms to document requests and related approvals; Review, evaluation, and approval of all documentation, hardware, software, and firmware change requests before changes occur; Document and archive authorizations for all modifications; An impact analysis to determine the effect of proposed changes on existing security controls, including required training needed to implement the control; Procedures for testing all changes before modifying the accredited production system so that new information security vulnerabilities are not introduced into the operational environment; Revise approvals, after testing and documentation, to migrate changes into the production environment; and Emergency change procedures and the personnel authorized to approve an emergency change. Emergency changes will be documented and approved by management, either prior to the change or after the fact. The configuration management plan also will specify procedures and documentation requirements for maintaining version control over production software and hardware, labeling and inventorying software, and distributing and implementing new or revised software.
Integrity controls	<ul style="list-style-type: none"> Integrity controls protect the system and the data it processes, stores, and/or transmits from accidental or malicious alteration or destruction and provide assurance to the end user that the information meets expectations about its quality and that it has not been altered. Validation controls are tests and evaluations used to determine compliance with security specifications and requirements. The system security requirements and controls that fall within this category are described in the following sections.
Virus control	<ul style="list-style-type: none"> AT&T understands anti-virus software is most effective when kept current. Therefore, the ISSO will verify that procedures for maintaining current anti-virus signatures are defined and implemented. AT&T emphasizes the protection of the support systems from viruses, worms, and other disruptive influences to maintain data integrity and availability. In support of this effort, AT&T takes the following steps with individual and corporate access equipment to service providing systems: <ul style="list-style-type: none"> Install the latest version of the corporate licensed anti-virus software designated by Network Security for AT&T use Options of automated anti-virus software to maintain current protections are not disabled or modified Run the anti-virus software on all local drives and all removable media maintained by the user Scan all network shares owned by the user

Control Requirement	Description
	<ul style="list-style-type: none"> — Scan all files that have been downloaded or copied from email messages or the Internet — Perform regular back-ups (preventing all data from being lost in case of pervasive virus or catastrophic attack) — Use only company authorized (i.e., purchased, owned, leased, or management-approved) software on company computers
Message integrity	<ul style="list-style-type: none"> ■ AT&T will support all Government efforts to protect the integrity of messages in transit where these messages are protected by encryption methods including site-to-site VPN or SSL/TLS VPN services. AT&T will also support the use reconciliation routines such as checksums, hash totals, or record counts to protect the receiver from malicious changes to a message by confirming a transmitted message has not been altered in transit as necessary.
Use of mobile code	<ul style="list-style-type: none"> ■ The system will be configured to prevent downloading mobile code or executable content if there is no requirement to do so. Downloading mobile code and executable content from a controlled interface between interconnected systems will be permitted only when boundary protection devices are appropriately configured and will be approved by the client agency. If mobile code or executable content is obtained via the web, the following will be applied: <ul style="list-style-type: none"> — All mobile code or executable content employed within the system will be approved by the ISSO or the GSA MTIPS AO. — A code review and quality control process for deploying mobile or executable content will be implemented and documented.
Documentation	<ul style="list-style-type: none"> ■ Documentation is a security control explaining how software/hardware is to be used and formalizes security and operational procedures specific to the system. System documentation includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to the automated information system security, including backup and contingency plans and descriptions of user and operator procedures. Typical system-related documentation is listed below: <ul style="list-style-type: none"> — A system security plan; — System-specific rules of behavior; — System risk assessment report; — Vendor-supplied documentation of purchased hardware and software; — Network diagrams and documentation on setups/configuration of routers and switches; — Justifications and management approval to use copyrighted software, shareware, or any personally owned software or equipment; — Application documentation for any in-house applications; — Software and hardware testing procedures and results; — Standard operating procedures for equipment and system interfaces; — User manuals; — Emergency procedures; — Configuration management plans; — Emergency change procedures such as procedures for emergency changes to system software; — Log of distribution and implementation of new or revised software; — The system contingency plan, including backup procedures; and — Written agreements regarding how data is shared between interconnected systems.
Security awareness and education	<ul style="list-style-type: none"> ■ Security awareness is communicated to Government users via Service Introduction Packets and Best Practices information brochures. The EIS subscriber website will include information about the MTIPS security policies, practices, and procedures. ■ AT&T vendors are contractually obligated to comply with company policy as well as Government requirements in support of the EIS contract. AT&T MTIPS security manager ensures that the appropriate vendor and contractor personnel are trained on the security policies and procedures as required. AT&T personnel who perform specific security roles, such as system administrator, security administrator, and database administrator, will undergo additional specialized training focused on their respective role. ■ In addition, all personnel with physical and/or logical access to a client agency's system will (1) receive the system rules of behavior, a copy of which will be signed and returned to the

Control Requirement	Description
	designated custodian, and (2) have access to applicable client agency security procedures and policies.
Incident response capability	<ul style="list-style-type: none"> ■ A formal incident response capability will be available and exercised at least annually. The capability and supporting procedures will be documented. The capability will include the following: <ul style="list-style-type: none"> — Security incident monitoring and tracking procedures, including (1) how to recognize and handle security incidents and (2) procedures for revising the incident handling procedures after an incident occurs. — System performance monitoring procedures to be used to analyze network performance logs in real time to look for availability problems, including active attacks. — Reporting to the appropriate emergency response. — Receiving and responding to alerts and advisories. A process will be developed to identify the sources of alerts and advisories to be monitored, the personnel responsible for monitoring and responding to alerts and advisories, and response guidance. — Designating the individual(s) responsible for testing and maintaining the incident response capability.

- **Technical Controls:** Technical controls are those executed by the computer system. Technical controls must be implemented to provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls always requires significant operational considerations and must be consistent with the management of security within the organization. **Table B-2.2-2** describes the types of control topics associated with operational controls. (NIST SP 800-37, Section 3.3, *RMF Step 3 — Implement Security Controls*)

Table B-2.2-2. Technical Control Topics. *Technical controls consist of the following requirements.*

Control Requirement	Description
Identification and authentication	<ul style="list-style-type: none"> ■ This section represents a scenario that typifies the Identification and Authentication section of an AT&T security plan. Off-the-shelf solutions will not be used for task orders under EIS, but will be customized to reflect the requirements of a specific system in a specific agency. ■ The first step is to determine the method of authentication and develop procedures and policies to enforce this method. For instance, if passwords are used, then the procedures and policies would be as follows: <ul style="list-style-type: none"> — The System Administrator issues the initial password; — The initial password expires at the time of its first use and the password owner must supply a new password; — Passwords cannot be the same as the user ID and must have at least three of the following: English uppercase, English lowercase, numerics, and special characters; — Minimum length of eight characters permitted; — Passwords expire every 90 days (enforced by the system); — Expired passwords disallowed after 6 generations; — User accounts disabled after no more than three consecutive invalid attempts (must be reinstated by an administrator); — Vendor-provided default passwords disabled or changed; — No shared accounts, including guest and training accounts, are defined; — No clear text display of passwords allowed on the screen; — Passwords stored as a hash or with one-way encryption;

Control Requirement	Description
	<ul style="list-style-type: none"> — System administrator passwords transmitted and stored with one-way encryption to prevent anyone from reading the clear-text version; — Passwords, IDs, or application user codes must not be entered in a file or record maintained in the system for the purpose of logging on automatically. ■ Depending on the system sensitivity, the agency's requirements for strong authentication and other factors, the customized security plan may specify stronger authentication tools, methods, and procedures (such as the use of one-time passwords).
Logical access control	<ul style="list-style-type: none"> ■ Logical access controls are the protection mechanisms that limit user's access to information and restrict their forms of system access to what is appropriate for them. These controls include policies that determine a user's level of system access, the procedures by which users are authorized appropriate access, the requirements for monitoring and maintaining access controls, and the system's technical features that enforce logical access controls.
User authorization	<ul style="list-style-type: none"> ■ Each user's access to an MTIPS system contracted to AT&T will be restricted to the fewest privileges that the user needs to perform their assigned duties. Where practical, critical functions will be divided among different individuals. When not practical, any variations from this requirement will be documented. There will be no shared administrative user accounts. Each privileged user has a personal account, so that all administrative activities are auditable. ■ There will be a formal process for requesting, establishing, issuing, and closing user accounts. An access control form will be developed to document access requests, justifications, and approvals. Compliance with requirements for least privilege, separation of duties, and unique accounts will be fully documented as part of the justification provided on the access control form. ■ A Government-designated individual must approve access privileges. The access control process requires this individual review the Access Control Lists not less than twice yearly to ensure that accesses are current and appropriate. All inactive accounts must be deleted to prevent unauthorized access and permissions must be changed to reflect any changes in a user's assigned duties.
Protection from unauthorized access	<ul style="list-style-type: none"> ■ For MTIPS and/or networks with firewall and/or IDS protection customized for that particular system or network, AT&T will describe the related measures to help protect the system in a secure enclave. ■ AT&T will identify any firewalls, IDS, and other devices installed to protect the system/network's perimeter. We will also describe the configuration of those devices. Generally, firewalls are to be configured to exclude any traffic except that which is specifically allowed. Any exceptions will be justified and documented. The IDS is to be configured to monitor site traffic for potential misuse or policy violations and recognize patterns of misuse, such as suspicious or unauthorized activity. ■ Other controls to protect MTIPS from unauthorized access include secure configuration of system devices by removing access to unneeded and unnecessary services from operating systems. Such unneeded or unnecessary services might include file transfer protocol (FTP), Telnet, compilers, and software development tools, if they are deemed to present security vulnerabilities in a specific situation.
Public access controls	<ul style="list-style-type: none"> ■ If a client agency's MTIPS task order provides for public access, AT&T will address the additional security controls needed to protect the integrity of the system and the confidence of the public in the system. Such controls include segregating information made directly accessible to the public from official agency records. Other controls AT&T has designed into Federal Government public-facing web sites include the following: <ul style="list-style-type: none"> — Some form of user identification and authentication — Digital signatures to enhance authentication — Access control to limit what the user can read, write, modify, or delete — Controls to prevent public users from modifying information on the system — CD-ROM for on-line storage of information for distribution — Verify programs and information distributed to the public are virus-free — Audit trails

Control Requirement	Description
Warning banner	<ul style="list-style-type: none"> ■ The Computer Fraud and Abuse Act of 1986 (Public Law 99-474) requires that a warning message be displayed notifying unauthorized users they have accessed a U.S. Government computer system and unauthorized use can be punished by fines or imprisonment. Although some Federal Government systems, such as FirstGov.gov, are intended for unrestricted use by the general public (a situation not prevalent when Public Law 99-474 was enacted), all systems that input, process, or store Government information must comply with the law. ■ Therefore, for all access to a Government system, with the exception of public requests for site content which will include the warning message cited in Section III.8, an approved agency warning banner will be displayed on all servers prior to user access, as required by NIST guidelines.
Audit trails	<ul style="list-style-type: none"> ■ To increase individual accountability, each user must have their own account, with a unique login ID and password (accounts must not be shared), and all privileged user activities will be logged so audit data will be available for review. Where possible, necessary administrator access must be granted through user accounts rather than through root access. ■ Since each user's security-related activities will be subject to recording and routine review for inappropriate activities, audit trails must be of sufficient detail to facilitate reconstructing events if compromise or malfunction occurs or is suspected. ■ AT&T defines that all resources to which access is controlled including applications and operating systems have the capability of generating security audit logs. All security logging mechanisms must be active from the first system initialization. These mechanisms include any automatic routines necessary to maintain the activity records and cleanup programs to ensure the integrity of the security audit/logging systems. ■ The audit logs will be secured. Access to online audit logs will be strictly controlled, preferably through separation of duties between system administrators who administer the access control function, for example, and those who administer the audit trail. AT&T will identify the individual(s) responsible for reviewing security activity logs and the frequency of their reviews. ■ Furthermore, the individuals responsible for information security will review the audit trail following a known system software problem, a known violation of existing requirements by a user, or any unexplained system or user problem. The individual(s) responsible for these audit-related tasks will be identified for each client agency task order. ■ Backup mechanisms and procedures exist to transport audit logs off the system prior to these logs being purged.

B-2.3 Implementation of Security Controls [C.2.8.4.5.2]

We review our systems thoroughly against the security controls approved by the GSA ISSO for MTIPS including those found in NIST SP 800-53, to determine how those controls need to be implemented. This includes the allocation of security controls, as discussed previously in **Section B-2.2**, into system-specific, common and hybrid controls. Additionally, while assembling a system's authorization package, the AT&T Information System Security Officer (ISSO) verifies that the security controls are applied appropriately to the related technology, based on how the system and sub-systems are implemented. In some cases, certain security controls will require additional components or technologies to be deployed. Additionally, some security controls may need to reference already implemented sub-systems of other controls, and in some

cases, certain security controls are not applicable based on how the system is designed and deployed.

B-2.4 Assessment of Security Control Effectiveness [C.2.8.4.5.2]

The effectiveness of the security controls against a deployed system can be determined by objectives for security control assessment within the Security Assessment Plan (SAP). The SAP describes what technologies and sub-systems are to be assessed and from this, the actual assessment will determine if there are any vulnerabilities or weaknesses of a system's technologies or sub-systems against the applicable security controls.

Based on the number and types of vulnerabilities, an assessor builds a risk posture for the system. The GSA AO or designated representative analyzes the risk posture to determine the effectiveness of the security controls for a given system. From that analysis, the GSA AO or designated representative decides whether or not to grant the system the authority to operate.

B-2.5 Authorization of the Information System [C.2.8.4.5.3; C.2.8.4.5.4(19-21, 24-27)]

The authorization of an information system depends on several factors:

- Security authorization package
- Plan of Actions and Milestones (POA&M)
- Risk determination of the system security platform
- Risk acceptance of the system security platform

Security Authorization Package: Our approach to assembling a security authorization package rests on the guidance in NIST Special Publication (SP) 800-53, Rev. 4, and GSA IT Security Procedural Guide 06-30, *Managing Enterprise Risk*. The process and deliverables consist of the following:

1. Categorize the system and document the results of the security categorization in the system security plan (SSP)
2. Describe the system, including system boundary, in the SSP
3. Register the system with appropriate organizational program/management offices
4. Identify the common controls and document them in the SSP

5. Select the system security controls and document them in the SSP
6. Develop a continuous monitoring strategy for monitoring security control effectiveness and any proposed/actual changes to the system and its environment of operation
7. Submit the system SSP to the GSA AO for review and approval
8. Implement the security controls specified in the SSP
9. Document the security control implementation, as appropriate, in the SSP providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs)
10. Develop a Security Assessment Plan (SAP) and submit to the GSA AO or their designee for review and approval
11. Assess the system security controls in accordance with the SAP
12. Prepare the security assessment report (SAR) to document any issues, findings, and recommendations from the security control assessment
13. Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate
14. Prepare a plan of action and milestones (POA&M) based on the SAR findings and recommendations, excluding any remediation actions taken; and
15. Assemble the security authorization package and submit it to the GSA AO for authorization.

The basic authorization package consists of the following deliverables:

- SSP
- SAR
- POA&M

The authorization package also includes additional documentation as follows:

- Any applicable Interconnection Security Agreements (ISAs)
- Control Tailoring Workbook
- System Design Document (SDD)
- NIST SP 800-53, Rev. 4, Control Summary Table
- Rules of Behavior (RoB)

- System Inventory
- Contingency Plan (CP), Disaster Recovery Plan (DRP), and Business Impact Assessment (BIA)
- Contingency Plan Test Plan (CPTP)
- Contingency Plan Test Report (CPTR)
- Privacy Impact Assessment (PIA)
- Configuration Management Plan (CMP) with System Baseline Configuration and EIS2020 information systems configuration settings
- Incident Response Plan (IRP)
- Incident Response Test Report (IRTR)
- Supply Chain Risk Management (SCRM) Plan
- Continuous Monitoring Plan (CMP)
- Vulnerability scan outputs, as appropriate
- Independent penetration test outputs, as appropriate [Section c.2.8.4.5.4 (20)]
- Code Review Report, as appropriate [Section C.2.8.4.5.4 (21)]
- Policy and Procedures documents including: [Section c.2.8.4.5.4 (27)]
 - Access Control Policy and Procedures (NIST SP 800-53 R4: AC-1)
 - Security Awareness and Training Policy and Procedures (NIST SP 800-53 R4: AT-1)
 - Audit and Accountability Policy and Procedures (NIST SP 800-53 R4: AU-1)
 - Security Assessment and Authorization Policies and Procedures (NIST SP 800-53 R4: CA-1)
 - Configuration and Management Policy and Procedures (NIST SP 800-53 R4: CM-1)
 - Contingency Planning Policy and Procedures (NIST SP 800-53 R4: CP-1)
 - Identification and Authentication Policy and Procedures (NIST SP 800-53 R4: IA-1)
 - Incident Response Policy and Procedures (NIST SP 800-53 R4: IR-1)
 - System Maintenance Policy and Procedures (NIST SP 800-53 R4: MA-1)
 - Media Protection Policy and Procedures (NIST SP 800-53 R4: MP-1)
 - Physical and Environmental Policy and Procedures (NIST SP 800-53 R4: PE-1)
 - Security Planning Policy and Procedures (NIST SP 800-53 R4: PL-1)
 - Personnel Security Policy and Procedures (NIST SP 800-53 R4: PS-1)

- Risk Assessment Policy and Procedures (NISTSP 800-53 R4: RA-1)
- Systems and Services Acquisition Policy and Procedures
(NIST SP 800-53 R4: SA-1)
- System and Communication Protection Policy and Procedures
(NIST SP 800-53 R4: SC-1)
- System and Information Integrity Policy and Procedures (NIST SP 800-53 R4: SI-1)

POA&M [C.2.8.4.5.4 (19)]: AT&T develops and maintains a system POA&M as directed by the GSA IT Security Procedural Guide 06-30, *Plan of Action and Milestones* (POA&M), and manages vulnerability scanning findings monthly and reports them with the POA&M quarterly, as required by the authorizing government program office.

This enables us to implement a compliant, orderly, approval process that yields risk and vulnerability statuses on an ongoing basis.

We develop the POA&M to document planned remedial actions to correct weaknesses or deficiencies from security assessments and continuous monitoring activities, including vulnerability scans. The POA&M captures the following elements:

- Weaknesses/vulnerabilities
- Milestone changes
- Point of contact for remediation
- Source that identified the
- Additional resources needed to support weakness/vulnerability
- remediation efforts
- Status
- Scheduled completion date

The AT&T system ISSO formats the POA&M, based on a template provided by the appropriate government organizational program/management office. To maintain accuracy and to meet the Government's periodic reporting requirements the POA&M is updated monthly.

The system ISSO updates and delivers the POA&M in the specified timeframe, based on the findings of the security control assessments and ongoing monitoring activities including vulnerability scanning. We include, in the quarterly POA&M submission, an action step to remediate high and medium items from scans and follow the GSA remediation timetable of 30 days to remediate high risk vulnerabilities and 90 days to remediate medium risk vulnerabilities [C.2.8.4.5.4 (24)]. The scan reports contain details

on any issues noted. The scan reports are available to the Government as part of the quarterly POA&M submission.

Risk Determination of the Security Platform: The determination of risk of a system or security platform is based on:

1. **Vulnerability**, i.e., what is the severity of the risk
2. **Impact**, i.e., what would it mean to us if the vulnerability were exploited
3. **Threat**, i.e., what is the likelihood of such an exploitation

After assessing each of the three risk factors and assigning them individual categories of: High, Medium or Low, they are then combined to obtain the overall risk assessment category:

1. High
2. Medium
3. Low

Risk Acceptance of the Security Platform: Either a panel or individuals within the GSA MTIPS organizational program/management office will review the system security authorization package for security risk. Based on their review and recommendations of the authorization package, the GSA MTIPS organizational program/management office AO determines the level of risk that the system represents and whether the risk is acceptable. If the GSA AO finds the risk level to be acceptable, then the official issues the Authorization to Operate (ATO).

Our MTIPS service currently holds an ATO granted by GSA. MTIPS follows the GSA guidance for a new security Accreditation and Authorization (A&A) to be performed on the system at least every three years or when there is a significant change to MTIPS that impacts the system's security posture, as well as an annual assessment in accordance with guidance from GSA. Additionally, all NIST SP 800-53 controls are tested and assessed every three years pursuant to maintaining the MTIPS ATO.

[C.2.8.4.5.3; C.2.8.4.5.4 (25); C.2.8.4.5.4 (26)]

B-2.6 Ongoing Monitoring of Security Controls and the Security State of the Information System [C.2.8.4.5.4; C.2.8.4.5.5]

Ongoing monitoring of security controls and security state of the information system consists of the following:

- Continuous monitoring of the system
- Logical maintenance of the system components
- Assessment of potential security impacts

Continuous Monitoring [C.2.8.4.5.4]: Post authorization of a system, the AT&T ISSO assembles a continuous monitoring report either every month or quarterly, based on the authorizing Government program office requirements for continuous monitoring, including any updates to relevant federal laws, directives, and policies. The report includes a POA&M, as discussed previously in **Section B-2.5**, which records any vulnerabilities in the system. Those vulnerabilities are assigned a risk level of high, medium or low.

Additionally, based on the types of vulnerabilities, the ISSO may assemble a plan of action to mitigate any vulnerabilities that appear to be patterns over time or for vulnerabilities that affect common system technologies or infrastructure.

Included in continuous monitoring are vulnerability scans that are performed on a monthly basis. [C.2.8.4.5.5 (2-3)] The scans are normally performed by the system owner but can also be carried out by a Government designee. In this case, AT&T will afford the Government designee logical and physical access to the systems and documentation that support MTIPS. For automated vulnerability scans, the Government can apply the following methods:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Authenticated and unauthenticated database application vulnerability scans
- Internal and external penetration testing

Additionally, automated scans can be performed by Government personnel or designees, using Government equipment and specified tools. However, the Government, at their discretion, can accept AT&T performed vulnerability scans and penetration tests in lieu of Government performed scans and tests.

Logical Maintenance: Our Information Technology Office (ITO) is charged with monitoring and maintaining the MTIPS systems to ensure those systems have the latest hardware deployed or software patches updated. The ISSO will alert ITO of hardware update or patch update requirements per the associated vulnerabilities in the POA&M. It is then up to ITO to test and implement any updates to mitigate those vulnerabilities. At no time during this process will AT&T publish or disclose the details of hardware or patch updates, or any safeguards designed or developed under a TO or otherwise provided by the Government, without written consent by the CO.

Assessment of Potential Security Impacts: Relative to the POA&M, the ISSO and ITO will monitor the types of vulnerabilities that impact the information system and determine if there may be potential for future security impacts. The vulnerabilities will be vetted to determine any potential threats to the information system and if any physical or logical changes to the system boundary are warranted.

If changes need to be made to the information system, the ISSO will request those changes from the system owner. When the changes are made by the system owner, the ISSO will then update the security authorization documentation, including the SSP, as to the proposed changes made or to be made to the information system. The ISSO will also alert the authorizing officer or designated representative of any changes made to the security authorization documentation for purposes of review and risk assessment.



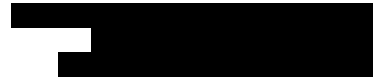
General Services Administration (GSA)

Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

GS00Q17NSD3000

Appendix C — Assumptions and Conditions



APPENDIX C — ASSUMPTIONS AND CONDITIONS [L.9]

C-1 Assumptions and Conditions [L.9]


In support of our proposal response, AT&T offers the following assumptions and/or conditions as listed and discussed in **Table C-1-1**. As required, this list identifies the area of the RFP affected by the assumption and/or condition, and details and documents our proposed resolution, as well as providing the area of the proposal affected. In response to RFP Section L.8 Exceptions, 





Table C-1-1. Volume 1 Assumptions and Conditions. *Technical Assumptions and Conditions are provided in order to support GSA's proposal evaluation process.*

#	Assumption or Condition	Area of the Proposal Affected	Area of the RFP Affected	Discussion	Resolution
					
					
					

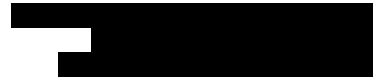


[REDACTED]

#	Assumption or Condition	Area of the Proposal Affected	Area of the RFP Affected	Discussion	Resolution
				[REDACTED]	
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED] C-3



#	Assumption or Condition	Area of the Proposal Affected	Area of the RFP Affected	Discussion	Resolution



Downloaded from <http://ajph.org/> on November 10, 2015