



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, March, 2025

Volume 2 – Management





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 2 — Management
March, 2025

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 2 — Management [L.30; L.11; L.9; M.2(2); M.2.2; G; E; J.2; C.3; D; F; H.10; H.35] 1

1 Management Response to Requirements for Section G: Contract

Administration Data [L.30(1); L.30.1(1); M.2(2); M.2.2; G; G.1] 1

1.1 AT&T's Approach and Capability to Provide User-Friendly, Compliant and Efficient Support Systems [L.30.1(1)(a); M.2.2(1 of 3); G]..... 2

1.1.1 Ordering [L.30.1(1)(a); M.2.2(1 of 3); G.3] 8

1.1.1.1 Fair Opportunity Process [G.3.1]..... 10

1.1.1.1.1 eBuy [G.3.1.1] 10

1.1.1.2 Task Orders [G.3.2]..... 10

1.1.1.3 Ordering Services [G.3.3]..... 11

1.1.1.3.1 General Requirements for Ordering Services [G.3.3.1]..... 13

1.1.1.3.2 Order Types [G.3.3.2] 14

1.1.1.3.3 Special Order Handling [G.3.3.3] 16

1.1.1.4 Testing and Acceptance of Services Ordered [G.3.4] 19

1.1.1.5 Performance Management [G.3.5]..... 20

1.1.2 Billing [L.30.1(1)(a); M.2.2(1 of 3); G.4] 20

1.1.2.1 Billing Prerequisites [G.4.1]..... 23

1.1.2.2 Direct Billing [G.4.2] 24

1.1.2.3 Billing Functional Requirements [G.4.3] 24

1.1.2.3.1 Adjustments [G.4.3.1]..... 25

1.1.2.3.2 Monthly Billing Informational Memorandum [G.4.3.2]..... 25

1.1.2.4 Disputes [G.4.4] 25

1.1.2.4.1 Billing Disputes Resolution [G.4.4.1]..... 25

1.1.2.5 Payment of a Bill by the Government [G.4.5] 26

1.1.2.6 Associated Government Fee [G.4.6]..... 26

1.1.2.7 General Billing Requirements 26

1.1.3 Business Support Systems [L.30.1(1)(a); M.2.2(1 of 3); G.5] 27

1.1.3.1 Overview [G.5.1] 31

1.1.3.2 Technical Requirements [G.5.3]..... 31

1.1.3.2.1 Web Interface [G.5.3.1] 32

1.1.3.2.2 Direct Data Exchange [G.5.3.2] 34

1.1.3.2.3 Role Based Access Control (RBAC) [G.5.3.3] 35

1.1.3.2.4 Data Detail Level [G.5.3.4]..... 36

1.1.3.3 BSS Component Service Requirements [G.5.4] 36

1.1.3.3.1 BSS Component Service Requirements Table [G.5.4.1]..... 36

1.1.3.4	BSS Development [G.5.5]	36
1.1.3.4.1	BSS Development and Implementation Plan [G.5.5]	36
1.1.3.4.2	BSS Change Control [G.5.5.1]	38
1.1.3.5	BSS Security Requirements [L.30.2.7; M.2.2(7 of 8); G.5.6]	38
1.1.3.6	Data Retention [G.5.7]	39
1.1.4	Customer Support Office and Technical Support [L.30.1(1)(a); M.2.2(1 of 3); G.6]	40
1.1.4.1	Customer Support Office [G.6.1]	40
1.1.4.2	Customer Support Office and Technical Support [G.6.2]	42
1.1.4.3	Supply Chain Risk Management [G.6.3]	44
1.1.4.3.1	Plan Submittal and Review [G.6.3.1]	44
1.1.5	Trouble Ticket Management [L.30.1(1)(a); M.2.2(1 of 3); G.6.4]	44
1.1.5.1	Trouble Ticket Management General Requirements [G.6.4.1]	45
1.1.5.2	[REDACTED]	46
1.1.6	Inventory Management [L.30.1(1)(a); M.2.2(1 of 3); G.7]	47
1.1.6.1	Inventory Management Process Definition [G.7.1]	48
1.1.6.1.1	Inventory Management Functional Requirements [G.7.1.1]	49
1.1.6.1.2	EIS Inventory Maintenance [G.7.1.2]	53
1.1.6.1.3	EIS Inventory Data Availability [G.7.1.3]	53
1.1.6.1.4	[REDACTED]	55
1.1.6.1.5	[REDACTED]	58
1.1.7	Service Level Management [L.30.1(1)(a); M.2.2(1 of 3); G.8]	58
1.1.7.1	Overview [G.8.1]	59
1.1.7.2	Service Level Agreement Tables [G.8.2]	59
1.1.7.2.1	[REDACTED]	60
1.1.7.2.2	[REDACTED]	62
1.1.7.2.3	[REDACTED]	64
1.1.7.3	[REDACTED]	64
1.1.7.3.1	[REDACTED]	64
1.1.7.3.2	[REDACTED]	65
1.1.7.3.3	[REDACTED]	65
1.1.7.4	[REDACTED]	65
1.1.7.4.1	Credit Management [G.8.4.1]	65
1.1.7.5	Service Level Reporting Requirements [G.8.5]	65
1.1.7.5.1	Report Submission [G.8.5.1]	65

1.1.7.5.2 Report Definitions [G.8.5.2]	65
1.1.8 Training [L.30.1(1)(a); M.2.2(1 of 3); G.10(1-6)]	66
1.1.8.1 Draft Customer Training Plan [G.10; F.2.1]	67
1.1.8.1.1 Training Curriculum [G.10.1]	68
1.1.8.1.2 Training Evaluation [G.10.2]	70
1.2 AT&T's Capability to Provide Customers with Web-Based Access to Support Systems [L.30.1(1)(b); M.2.2(2 of 3); G.5]	70
2 Management Response to Requirements for Section E: Inspection and Acceptance [L.30(2); L.30.1(2); E]	71
2.1 AT&T Capability to Comply with the Requirements in Section E: Inspection and Acceptance [L.30.1(2)]	71
2.1.1 FAR 52.252 Clauses Incorporated by Reference (Feb 1998) [E.1.1]	72
2.2 Test Methodology [E.2]	72
2.2.1 Business Support Systems Verification Testing [E.2.1]	73
2.2.1.1 Scope [E.2.1.1]	75
2.2.1.2 BSS Test Scenarios [E.2.1.2]	75
2.2.1.2.1 Testing Prerequisites [E.2.1.2.1]	75
2.2.1.2.2 Test Scenarios [E.2.1.2.2]	75
2.2.1.3 BSS Test Cases [E.2.1.3]	76
2.2.1.4 Test Results [E.2.1.4]	77
2.2.1.5 Deliverables [E.2.1.5-E.2.1.5.2]	77
2.2.2 EIS Services Verification Testing [E.2.2]	77
2.2.2.1 General Testing Requirements [E.2.2.1]	78
2.2.2.2 Test Scenarios [E.2.2.2; E.2.2.2.1]	78
2.2.2.3 Test Cases [E.2.2.3]	79
2.2.2.4 Test Data Sets [E.2.2.4]	79
2.2.2.5 Test Results and Acceptance [E.2.2.5]	79
2.2.2.6 Deliverables [E.2.2.6]	79
3 Management Response to Requirements for Section J.2: Contractor Data Interaction Plan [L.30(3); L.30.1(3); M.2.2(3 of 3); J.2]	79
3.1 AT&T's Capability to Comply with Section J.2: Contractor Data Interaction Plan [L.30.1(3)]	79
3.1.1 EIS Management and Operations: High-Level Process Diagram [J.2.1.1]	80
3.2 Common Data Interaction Requirements [J.2.2]	81
3.3 Task Order Data Management [J.2.3]	82
3.3.1 Common Operational Requirements [J.2.3.1]	83
3.3.2 Task Order Data Management Process [J.2.3.2]	83

3.3.3	Deliverables and Data Exchange [J.2.3.3]	84
3.4	Ordering [J.2.4]	84
3.4.1	Common Operational Requirements [J.2.4.1]	84
3.4.2	Ordering Process [J.2.4.2]	86
3.4.3	Deliverables and Data Exchange [J.2.4.3]	87
3.5	Billing [J.2.5]	87
3.5.1	Common Operational Requirements [J.2.5.1]	88
3.5.2	Billing Process [J.2.5.2]	89
3.5.3	Deliverables and Data Exchange [J.2.5.3]	90
3.6	Disputes [J.2.6]	90
3.7	Inventory Management [J.2.7]	91
3.8	SLA Management [J.2.8]	92
3.9	Data Transfer Mechanisms [J.2.9]	94
3.10	Data Dictionary [J.2.10]	95
3.10.1	Common Data Requirements [J.2.10.1]	95
3.10.2	Data Set Content [J.2.10.2]	97
3.10.2.1	Data Sets: Primary Data [J.2.10.2.1]	97
3.10.2.2	Data Sets: Reference Data [J.2.10.2.2]	99
3.10.2.3	Data Sets: Task Order Data [J.2.10.2.3]	99
3.10.3	Data Element Specifications [J.2.10.3]	100
APPENDIX A — Program Management Plan (PMP) [L.30; L.30.2.1; M.2.2 (3 of 3); G.9.4; C.3; H.10; H.35; D; F]		A-1
A-1	Summary of Contract Management Requirements, Including Government Dependencies and Assumptions [L.30.2.1(1); G.9.4(1)]	A-2
A-2	Summary Description of Service Solution [L.30.2.1(2); G.9.4(2)]	A-4
A-2.1	Methodology to Comply with Service Ordering Requirements [L.30.2.1(2); G.9.4(2)]	A-4
A-2.2	Methodology to Comply with Billing Requirements [L.30.2.1(2); G.9.4(2)]	A-6
A-2.3	Methodology to Comply with Inventory Management Requirements [L.30.2.1(2); G.9.4(2)]	A-7
A-2.4	Methodology to Comply with Service Management Requirements [L.30.2.1(2); G.9.4(2)]	A-8
A-3	Draft Program Management Schedule [L.30.2.1(3); G.9.4(3)]	A-10
A-4	Draft Transition Management Approach, Including Project Management Process, Procedures, and Tools To Meet the Transition Requirements in Section C.3 [L.30.2.1(4); G.9.4(4); C.3-C.3.3.4]	A-13
A-4.1	Transition Project Management [L.30.2.1(4)(a); G.9.4(4)(a)]	A-15

A-4.1.1	Billing, Service Ordering, Trouble Reporting, and Customer Service Processes That Are Unique for Transitioning onto EIS and off EIS [L.30.2.1(4)(a); G.9.4(4)(a)]	A-19
A-4.1.2	How AT&T will Expedite Transition When AT&T Is Also the Incumbent Service Provider [L.30.2.1(4)(a); G.9.4(4)(a)]	A-22
A-4.1.3	AT&T Will Coordinate with Other Incumbent Providers to Ensure a Smooth, Successful, and Timely Transition [L.30.2.1(4)(a); G.9.4(4)(a)]	A-23
A-4.1.4	Identification and Assessment of the Major Transition Risks and the Proposed Response to Each [L.30.2.1(4)(a); G.9.4(4)(a)]	A-23
A-4.2	Agency Solicitations [L.30.2.1(4)(b); G.9.4(4)(b)]	A-24
A-4.2.1	Approach to Assisting Agencies with Selecting New or Enhanced Services to Replace Services on Expiring Contracts [L.30.2.1(4)(b); G.9.4(4)(b)]	A-25
A-4.2.2	Incentives to Expedite Transition [L.30.2.1(4)(b); G.9.4(4)(b)]	A-26
A-4.3	Customer Support During Transition [L.30.2.1(4)(c); G.9.4(4)(c)] ...	A-26
A-4.3.1	Describe and Provide An Outline for Any Transition Handbooks or Guides that AT&T Will Make Available to Customers [L.30.2.1(4)(c); G.9.4(4)(c)]	A-27
A-4.3.2	Provide Target Date for Publication [L.30.2.1(4)(c); G.9.4(4)(c)]	A-27
A-4.4	Interconnection Plan [L.30.2.1(4)(d); G.9.4(4)(d)]	A-27
A-4.4.1	Description of Interconnection Arrangements Between the Incumbent Contractor's Network and the EIS Networks during the Transition, Including the Interconnection Arrangements with the Local Exchange Network, the IXCs, and Government Private Networks [L.30.2.1(4)(d); G.9.4(4)(d)]	A-27
A-4.4.2	Description of Any Interconnections with Other Service Providers, Including Other Operating Units Within AT&T Such As Wholesale Services, Known or Expected to be Required to Transition Services [L.30.2.1(4)(d); G.9.4(4)(d)]	A-28
A-4.4.3	Potential Impact to Customers' Operations [L.30.2.1(4)(d); G.9.4(4)(d)]	A-28
A-4.5	Transition Contingency Plan [L.30.2.1(4)(e); G.9.4(4)(e)]	A-29
A-4.6	Additional Areas Proposed by AT&T [G.9.4(4)]	A-30
A-5	Resource Plan [L.30.2.1(5); G.9.4(5)]	A-30

A-5.1	Financial Resources [L.30.2.1(5)(a); G.9.4(5)(a)]	A-30
A-5.2	Human Resources [L.30.2.1(5)(b); G.9.4(5)(b)]	A-32
A-5.3	Equipment [L.30.2.1(5)(c); G.9.4(5)(c)]	A-34
A-6	Quality Control Program [L.30.2.1(6); G.9.4(6)]	A-36
A-6.1	Management Approach for Formulating and Enforcing Work and Quality Standards [L.30.2.1(6); G.9.4(6); G.9.2]	A-37
A-6.2	Management Approach for Ensuring Compliance with Contractual Service Level Agreements (SLAs) [L.30.2.1(6); G.9.4(6)]	A-39
A-6.3	Management Approach for Reviewing Work in Progress [L.30.2.1(6); G.9.4(6)]	A-39
A-6.4	Management Approach for Providing Customer Support Services [L.30.2.1(6); G.9.4(6)]	A-40
A-7	Key Personnel and Organizational Structure [L.30.2.1(7); G.9.4(7)]	A-40
A-7.1	Management Structure, Organizations, and Roles and Responsibilities of Each Component That Performs Work Under the Contract [L.30.2.1(7); G.9.4(7)]	A-41
A-7.2	[REDACTED]	A-42
A-7.2.1	Key Personnel [L.30.2.1(7); H.10.1 – H.10.1(d)]	A-43
A-7.2.2	Corporate/Organizational Structure [L.30.2.1(7); H.10.3]	A-44
A-8	Risk Management [L.30.2.1(8); G.9.4(8)]	A-53
A-8.1	Process for Identifying Program Risks, Including Risks Identified in the Contract and Actions to Mitigate them [L.30.2.1(8); G.9.4(8)]	A-55
A-9	Information Systems [L.30.2.1(9); G.9.4(9)]	A-59
A-9.1	Description of the BSS Employed to Implement the Requirements of the Contract [L.30.2.1(9); M.2.2(3); G.9.4(9)]	A-60
A-9.1.1	Consistency with Security Plans to Prevent Unauthorized Access to the Government's Data [L.30.2.1(9); G.9.4(9)]	A-61
A-9.1.2	Consistency with Security Plans to Prevent Access by An Agency to Data Belonging to Any Other Agency [L.30.2.1(9); G.9.4(9)]	A-64
A-9.2	Description of How AT&T Will Ensure Systems Are Available to Meet the Requirements of Business Support Systems [L.30.2.1(9); G.9.4(9)]	A-64
A-10	Additional Elements of the Program Management Approach [L.30.2.1]	A-65
A-10.1	Personnel Security [H.35]	A-65
A-10.2	Deliverables and Reports [D; F]	A-66
A-11	Summary	A-67

APPENDIX B — SCRM Plan [L.30; L.30.2.2; M.2.2 (1 of 7); G.6.3]	B-1
B-1 AT&T's Approach to SCRM [L.30.2.2; G.6.3]	B-3
B-2 Demonstration of How AT&T's Approach Will Reduce and Mitigate Supply Chain Risks [L.30.2.2; G.6.3]	B-6
B-3 Management of Supply Chain Risk throughout Each of the Five Supply Chain Phases [L.30.2.2; G.6.3]	B-6
B-3.1 Design and Engineering [L.30.2.2(1 of 5); G.6.3(1 of 5)]	B-8
B-3.2 Manufacturing and Assembly [L.30.2.2(2 of 5); G.6.3(2 of 5)]	B-9
B-3.3 Distribution and Warehousing [L.30.2.2(3 of 5); G.6.3(3 of 5)]	B-9
B-3.4 Operations and Support [L.30.2.2(4 of 5); G.6.3(4 of 5)]	B-9
B-3.5 Disposal and Return [L.30.2.2(5 of 5); G.6.3(5 of 5)]	B-10
B-4 Mandatory SCRM Requirements That Addresses Counterfeit and Illegally Modified Products [L.30.2.2; G.6.3]	B-10
B-4.1 How AT&T Ensures that Requirements for Genuine Information Technology Tools (ITT) Are Imposed [L.30.2.2(1 of 11); G.6.3(1)]	B-11
B-4.1.1 AT&T's Reasonable Steps to Ensure Its SCRM Plan Is Performed for ITT in Its Delivered and Installed Configuration [L.30.2.2(1 of 11)(a); G.6.3(1)(a)]	B-11
B-4.1.2 Equipment Reseller Licensing for OEM Equipment and Software [L.30.2.2(1 of 11)(b); G.6.3(1)(b)]	B-11
B-4.1.3 ITT OEM Exercise of Strict Quality Control [L.30.2.2(1 of 11)(c); G.6.3(1)(c)]	B-11
B-4.1.4 AT&T's Traceability of Assurance and Evidence of Genuineness of ITT Back to the Licensed Product and Component OEMs [L.30.2.2(1 of 11)(d); G.6.3(1)(d)]	B-12
B-4.2 AT&T's Use of System Security Engineering Processes [L.30.2.2(2 of 11); G.6.3(2)]	B-12
B-4.2.1 Protection Against External Threats [L.30.2.2(2 of 11); G.6.3(2)]	B-12
B-4.2.2 Protection Against Hardware and Software Vulnerabilities [L.30.2.2(2 of 11); G.6.3(2)]	B-12
B-4.3 AT&T's Strategy for Implementing SCRM Security Requirements [L.30.2.2(3 of 11); G.6.3(3)]	B-13
B-4.3.1 Security Controls Described in NIST [L.30.2.2(3 of 11); G.6.3(3)]	B-15
B-4.3.2 Implementation of the Controls Tailored in Scope to the Effort and the Specific Information [L.30.2.2(3 of 11); G.6.3(3)]	B-15
B-4.4 Criticality Analysis (CA) Process Used by AT&T [L.30.2.2(4 of 11); G.6.3(4)]	B-15

B-4.4.1	Description of AT&T's Supply Chain [L.30.2.2(4 of 11); G.6.3(4)].....	B-15
B-4.4.2	All Critical Hardware and Software Components (and Material Included in Products) [L.30.2.2(4 of 11); G.6.3(4)].....	B-16
B-4.4.3	Key Suppliers [L.30.2.2(4 of 11); G.6.3(4)].....	B-16
B-4.4.4	Proof of Company Ownership and Location for Key Suppliers and Component Manufacturers [L.30.2.2(4 of 11); G.6.3(4)].....	B-16
B-4.5	How AT&T Ensures That Products and Components Are Not Repaired and Shipped as New Products and Components to the Government [L.30.2.2(5 of 11); G.6.3(5)].....	B-17
B-4.6	How AT&T Ensures That Supply Channels Are Monitored for Counterfeit Products Throughout the Product Life Cycle to Include Maintenance and Repair [L.30.2.2(6 of 11); G.6.3(6)]	B-18
B-4.7	How AT&T's Physical and Logical Delivery Mechanisms Protect Against Unauthorized Access, Exposure of System Components, Information Misuse, Unauthorized Modification, or Redirection [L.30.2.2(7 of 11); G.6.3(7)]	B-18
B-4.8	How AT&T's Operational Processes and Disposal Processes Limit Opportunities for Knowledge Exposure, Data Release, or System Compromise [L.30.2.2(8 of 11); G.6.3(8)]	B-20
B-4.9	Identification of the Relationship Between AT&T and the Manufacturer [L.30.2.2(9 of 11); G.6.3(9)]	B-20
B-4.10	AT&T's Expressed Warranty [L.30.2.2(10 of 11); G.6.3(10)]	B-21
B-4.11	How AT&T Ensures Independent Verification and Validation of Assurances and Provides Supporting Evidence as Required [L.30.2.2(11 of 11); G.6.3(11)]	B-21
B-5	Inclusion of Information Requirement (G.6.3) in Subcontracts at All Tiers [L.30.2.2; G.6.3].....	B-21
B-6	Identification of All Subcontractors Providing Critical Components or Services and Requirement for Information Necessary to Complete the SCRM Plan [L.30.2.2; G.6.3].....	B-22
B-7	Compliance with NIST SP 800-161 Supply Chain Risk Management Practices [L.30.2.2; G.6.3].....	B-22
B-8	SCRM Plan Updates [L.30.2.2; G.6.3]	B-23
B-9	Plan Submittal and Review [G.6.3.1]	B-24
APPENDIX C — Draft BSS Verification Test Plan].....		C-1
C-1	Scope [L.30.2.3; E.2.1.1]	C-3
C-1.1	BSS Testing Verification That All BSS Functional, Regression, Load, and Security Requirements Have Been Successfully Met [L.30.2.3(1); E.2.1.1]	C-4

C-1.2	[REDACTED]	C-5
C-1.2.1	[REDACTED]	C-5
C-1.2.2	[REDACTED]	C-6
C-1.2.3	[REDACTED]	C-6
C-1.2.4	[REDACTED]	C-6
C-1.2.5	[REDACTED]	C-6
C-1.2.6	[REDACTED]	C-7
C-1.3	[REDACTED]	C-7
C-1.4	BSS Testing's Inclusion of Multiple Test Cases [L.30.2.3(4); E.2.1.1]	C-8
C-1.5	[REDACTED]	C-8
C-1.6	Observance of BSS Verification Testing by Government Representatives [E.2.1.1]	C-8
C-1.7	Performance of BSS Verification Testing [E.2.1.1]	C-9
C-2	BSS Test Scenarios [E.2.1.2]	C-9
C-2.1	[REDACTED]	C-9
C-2.2	[REDACTED]	C-9
C-3	[REDACTED]	C-12
C-3.1	[REDACTED]	C-14
C-3.2	[REDACTED]	C-16
C-3.3	[REDACTED]	C-16
C-3.4	[REDACTED]	C-18
C-3.5	[REDACTED]	C-23
C-3.6	[REDACTED]	C-26
C-3.7	BSS-TS07: Rapid Provisioning & Self-Provisioning Orders [E.2.1.3.7]	C-26
C-3.8	[REDACTED]	C-28
C-3.9	[REDACTED]	C-30
C-3.10	[REDACTED]	C-30
C-3.11	[REDACTED]	C-31
C-3.12	BSS-TS12: Regression Testing [E.2.1.3.12]	C-32
	C-3.12.1 BSS-TS12-01: Regression Testing [E.2.1.3.12.1]	C-32
C-3.13	BSS-TS13: Security Testing [E.2.1.3.13]	C-32
	C-3.13.1 BSS-TS13-01: Security Testing [E.2.1.3.13.1]	C-32
C-4	[REDACTED]	C-33
C-4.1	Functional Requirements Processes [E.2.1.4]	C-33

C-4.1.1	[REDACTED]	C-33
C-4.1.2	[REDACTED]	C-33
C-4.1.3	[REDACTED]	C-33
C-4.1.4	[REDACTED]	C-33
C-4.1.5	[REDACTED]	C-34
C-4.1.6	[REDACTED]	C-34
C-4.2	[REDACTED]	C-34
C-4.3	[REDACTED]	C-35
C-4.4	[REDACTED]	C-35
C-4.5	[REDACTED]	C-36
C-4.6	[REDACTED]	C-36
C-4.7	[REDACTED]	C-36
C-5	[REDACTED]	C-36
C-5.1	[REDACTED]	C-36
C-5.2	[REDACTED]	C-37

APPENDIX D — EIS Services Verification Test Plan (EIS Test Plan) [L.30; L.30.2.4; M.2.2(3 of 7); E.2.2]..... D-1

D-1	Service Area—Data Service	D-4
D-1.1	EIS Test Plan for Virtual Private Network Service (MANDATORY) [L.30.2.4; E.2.2]	D-4
D-1.2	EIS Test Plan for Ethernet Transport Service (MANDATORY) [L.30.2.4; E.2.2]	D-7
D-1.3	EIS Test Plan for Optical Wavelength Service (OPTIONAL) [L.30.2.4; E.2.2]	D-9
D-1.4	EIS Test Plan for Private Line Service (OPTIONAL) [L.30.2.4; E.2.2]	D-11
D-1.5	EIS Test Plan for Synchronous Optical Network Service (OPTIONAL) [L.30.2.4; E.2.2]	D-14
D-1.6	EIS Test Plan for Dark Fiber Service (OPTIONAL) [L.30.2.4; E.2.2]	D-16
D-1.7	EIS Test Plan for Internet Protocol Service (OPTIONAL) [L.30.2.4; E.2.2]	D-18
D-1.8	[REDACTED]	D-20
D-2	Service Area: Voice Service	D-23

D-2.1	Internet Protocol Voice Service (VOICE MANDATORY) [L.30.2.4; E.2.2]	D-23
D-2.2	[REDACTED]	D-25
D-2.3	EIS Test Plan for Toll Free Service (OPTIONAL) [L.30.2.4; E.2.2] ..	D-27
D-2.4	EIS Test Plan for Circuit Switched Data Service (OPTIONAL) [L.30.2.4; E.2.2]	D-29
D-3	Service Area: Contact Center Service	D-30
D-3.1	EIS Test Plan for Contact Center Service (OPTIONAL) [L.30.2.4; E.2.2]	D-30
D-4	Service Area: Colocated Hosting Service	D-32
D-4.1	EIS Test Plan for Data Center Service/Colocated Hosting Service (OPTIONAL) [L.30.2.4; E.2.2]	D-32
D-5	Service Area: Cloud Service	D-33
D-5.1	[REDACTED]	D-33
D-5.2	EIS Test Plan for Platform as a Service (OPTIONAL) [L.30.2.4; E.2.2]	D-34
D-5.3	EIS Test Plan for Software as a Service (OPTIONAL) [L.30.2.4; E.2.2]	D-36
D-5.4	EIS Test Plan for Content Delivery Network Service (OPTIONAL) [L.30.2.4; E.2.2]	D-37
D-6	Service Area: Wireless Service	D-39
D-6.1	EIS Test Plan for Wireless Service (OPTIONAL) [L.30.2.4; E.2.2] ..	D-39
D-7	[REDACTED]	D-40
D-7.1	[REDACTED]	D-40
D-7.2	[REDACTED]	D-42
D-8	Service Area: Managed Service	D-44
D-8.1	EIS Test Plan for Managed Network Service (MANDATORY) [L.30.2.4; E.2.2]	D-44
D-8.2	EIS Test Plan for Web Conferencing Service (OPTIONAL) [L.30.2.4; E.2.2]	D-45
D-8.3	EIS Test Plan for Unified Communications Service (OPTIONAL) [L.30.2.4; E.2.2]	D-46
D-8.4	EIS Test Plan for Managed Trusted Internet Protocol Service (OPTIONAL) [L.30.2.4; E.2.2]	D-48
D-8.5	EIS Test Plan for Managed Security Service (OPTIONAL) [L.30.2.4; E.2.2]	D-52

D-8.6	EIS Test Plan for Managed Mobility Service (OPTIONAL) [L.30.2.4; E.2.2]	D-55
D-8.7	EIS Test Plan for Audio Conferencing Service (OPTIONAL) [L.30.2.4; E.2.2]	D-58
D-8.8	EIS Test Plan for Video Teleconferencing Service (OPTIONAL) [L.30.2.4; E.2.2]	D-59
D-8.9	EIS Test Plan for DHS Intrusion Prevention Security Service (OPTIONAL) [L.30.2.4; E.2.2]	D-61
D-8.10	EIS Test Plan for Software Defined Wide Area Network Service (OPTIONAL) [L.30.2.4; E.2.2]	D-63
D-9	Service Area: Access Arrangements [C.1.8.1] (MANDATORY COMPONENT)	D-64
D-9.1	EIS Test Plan for Access Arrangements [L.30.2.4; E.2.2]	D-64
D-10	Service Area: Service Related Equipment [C.1.8.1]	D-64
D-10.1	EIS Test Plan for Service Related Equipment (OPTIONAL) [L.30.2.4; E.2.2]	D-64
D-11	Service Area: Service Related Labor [C.1.8.1]	D-64
D-11.1	EIS Test Plan for Service Related Labor [L.30.2.4; E.2.2]	D-64
D-12	Service Area: Cable and Wiring [C.1.8.1]	D-64
D-12.1	EIS Test Plan for Cable and Wiring [L.30.2.4; E.2.2]	D-64
APPENDIX E — Climate Risk Management Plan [L.30; L.30.2.5; M.2.2 (4 of 7); G.12] 1		
E-1	Climate Change Adaptation [G.12.1]	E-3
E-2	Sustainability and Green Initiatives [G.12.2]	E-7
E-2.1	Electronic Product Environmental Assessment Tool [G.12.2.1]	E-14
E-2.2	Energy Efficient Products [G.12.2.2]	E-14
E-2.3	Data Centers and Cloud Services [G.12.2.3]	E-16
APPENDIX F — Financial Status Report (Sample) [L.30; L.30.2.6; M.2.2(5 of 7); G.9.5] F-1		
APPENDIX G — Business Support Systems (BSS) Risk Management Framework Plan [L.30; L.27.2; L.30.2.7; M.2.2.7; G.5.6; G.5.6.4; (2, 2a)] G-1		
G-1	General Security Compliance Requirements [G.5.6.1]	G-1
G-2	GSA Security Compliance Requirements [G.5.6.2]	G-1
G-3	Security Assessment and Authorization (Security A&A) [G.5.6.3]	G-1
G-4	BSS System Security Plan (SSP) [G.5.6.4]	G-5
G-4.1	Security Assessment Boundary and Scope Document (BSD) [G.5.6.4(1)]	G-6
G-4.2	Interconnect Security Agreements [G.5.6.4(2)]	G-7
G-4.3	Control Tailoring Workbook [G.5.6.4(3)]	G-9

G-4.4	GSA Control Summary Table for a Moderate Impact Baseline [G.5.6.4(4)]	G-9
G-4.5	Rules of Behavior [G.5.6.4(5)]	G-10
G-4.6	System Inventory [G.5.6.4(6)]	G-10
G-4.7	Contingency Plan [G.5.6.4(7)]	G-11
G-4.7.1	Disaster Recovery Plan (DRP) [G.5.6.4(7).1]	G-12
G-4.7.2	Business Impact Assessment (BIA) [G.5.6.4(7).2]	G-13
G-4.8	Contingency Plan Test Plan (CPTP) [G.5.6.4(8)]	G-14
G-4.9	Contingency Plan Test Report [G.5.6.4(9)]	G-14
G-4.10	Privacy Impact Assessment (PIA) [G.5.6.4(10)]	G-15
G-4.11	Configuration Management Plan [G.5.6.4(11)]	G-16
G-4.12	System(s) Baseline Configuration Standard Document [G.5.6.4(12)]	G-16
G-4.13	System Configuration Settings [G.5.6.4(13)]	G-17
G-4.14	Incident Response Plan (IRP) [G.5.6.4(14)]	G-18
G-4.15	Incident Response Test Report (IRTR) [G.5.6.4(15)]	G-19
G-4.16	Continuous Monitoring of Security Controls of AT&T's System with a Continuous Monitoring Plan [G.5.6.4(16)]	G-19
G-4.17	Plan of Action and Milestones [G.5.6.4(17)]	G-21
G-4.18	Independent Penetration Test Report [G.5.6.4(18)]	G-22
G-4.19	Code Analysis Reviews with Code Review Report [G.5.6.4(19)]	G-22
G-4.20	Security/Risk Assessment and Penetration Tests [G.5.6.4(20)]	G-23
G-4.21	Security/Risk Assessment Report (SAR) [G.5.6.4(21)]	G-23
G-4.22	Mitigation of Security Risks [G.5.6.4(22)]	G-24
G-4.23	Annual FISMA Assessment [G.5.6.4(23)]	G-24
G-4.24	Policy and Procedure Documents [G.5.6.4(24)]	G-25
G-5	Additional Security Requirements [G.5.6.6; Section I]	G-26
G-5.1	Personnel Security Suitability [G.5.6.6.1; Section I]	G-28

APPENDIX H — NS/EP Functional Requirements Implementation Plan [L.30; L.30.2.8; M.2.2 (7 of 7); G.11]		H-1
H-1	Basic Functional Requirements [G.11.1]	H-3
H-1.1	Enhanced Priority Treatment [G.11.1(1)]	H-4
H-1.2	Secure Networks [G.11.1(2)]	H-4
H-1.3	Non-Traceability [G.11.1(3)]	H-5
H-1.4	Restorability [G.11.1(4)]	H-6
H-1.5	International Connectivity [G.11.1(5)]	H-7
H-1.6	Interoperability [G.11.1(6)]	H-7
H-1.7	Mobility [G.11.1(7)]	H-8

H-1.8	Nationwide Coverage [G.11.1(8)]	H-8
H-1.9	Survivability/Endurability [G.11.1(9)]	H-9
H-1.10	[REDACTED]	H-
H-1.11	Broadband Service [G.11.1(11)]	H-10
H-1.12	Scalable Bandwidth [G.11.1(12)]	H-10
H-1.13	Affordability [G.11.1(13)]	H-11
H-1.14	Reliability/Availability [G.11.1(14)]	H-11
H-2	Protection of Classified and Sensitive Information [G.11.2]	H-12
H-3	Department of Homeland Security Emergency Communications Division	
	Priority Telecommunications Services [G.11.3]	H-12
H-3.1	Government Emergency Telecommunications Service [G.11.3.1]..	H-13
H-3.2	Wireless Priority Service [G.11.3.2]	H-19
H-3.3	Telecommunication Service Priority [G.11.3.3]	H-20
APPENDIX I..... — VOLUME 2 ASSUMPTIONS AND CONDITIONS [L.9]		I-1
I-1	Assumptions and Conditions [L.9]	I-1

LIST OF FIGURES

Figure 1-1. Elements for Success.....	1
Figure 1.1-1. [REDACTED].....	4
Figure 1.1-2. [REDACTED].....	5
Figure 1.1-3. [REDACTED].....	5
Figure 1.1-4. [REDACTED].....	6
Figure 1.1.1-1. Fair Opportunity Process.....	10
Figure 1.1.1-2. Service Order Flow.....	11
Figure 1.1.1-3. AT&T to GSA/Agencies Ordering Data Interchange.....	13
Figure 1.1.1-4. Task Order Project.....	18
Figure 1.1.2-1. Enhanced Billing Capabilities on EIS.....	20
Figure 1.1.2-2. AT&T EIS Billing Process Flow.....	21
Figure 1.1.2-3. Billing Menu Options.....	22
Figure 1.1.2-4. Integrated Billing View.....	27
Figure 1.1.3-1. [REDACTED].....	29
Figure 1.1.3-2. [REDACTED].....	30
Figure 1.1.3-3. [REDACTED].....	32
Figure 1.1.3-4. [REDACTED].....	34
Figure 1.1.3-5. AT&T's Continuous Delivery Process.....	37
Figure 1.1.3-6. AT&T BSS Development, Test and Implementation timeline.....	38
Figure 1.1.4-1. [REDACTED].....	41
Figure 1.1.4-2. [REDACTED].....	41
Figure 1.1.4-3. EIS CSO is Easy to Contact.....	42
Figure 1.1.4-4. [REDACTED].....	43
Figure 1.1.5-1. [REDACTED].....	44
Figure 1.1.6-1. [REDACTED].....	48
Figure 1.1.6-2. [REDACTED].....	49
Figure 1.1.6-3. [REDACTED].....	53
Figure 1.1.6-4. [REDACTED].....	56
Figure 1.1.6-5. AT&T Internal Audits.....	57
Figure 1.1.6-6. EIS Inventory Reconciliation Report.....	58
Figure 1.1.7-1. [REDACTED].....	59
Figure 1.1.8-1. AT&T Training Approach.....	68
Figure 2.2.1-1. Testing Process Flow.....	74
Figure 2.2.2-1. Verification Testing and Service Order Process.....	78
Figure 3.1-1. CDIP High-Level Process Flow.....	81

Figure 3.3-1. CDIP-Task Order. Data Management Process Flow. <i>Automated and highly secure transfer of Task Order data is fully compliant with EIS requirements and cover the three categories of data exchanged</i>	82
Figure 3.3-2. Task Order Data Management Process	83
Figure 3.4-1. Order Data Interchange Flow	84
Figure 3.4-2. Typical Order Flow	86
Figure 3.5-1. CDIP-Billing Process Flow	88
Figure 3.6-1. CDIP-Billing Process Flow	91
Figure 3.7-1. CDIP-Inventory Process Flow	92
Figure 3.8-1. CDIP-SLA Management Process Flow	93
Figure 3.10-1. CDIP-Task Order Data Management Process Flow	95
Figure 3.10.3-1. Elements for Success	101
Figure A-2-1. AT&T Portal and BSS	A-4
Figure A-3-1. Draft Program Management Schedule	A-11
Figure A-3-2. Schedule to Achieve ATO	A-11
Figure A-3-3. BSS Testing and Validation Schedule	A-12
Figure A-3-4. FISMA Approval Timeline	A-12
Figure A-4-1. Transition Project Management Process	A-13
Figure A-4-2. Transition Project Management Procedures	A-14
Figure A-4-3. Transition Project Management Tools	A-14
Figure A-4.1-1. [REDACTED]	A-16
Figure A-4.1.4-1. Principle Transition Risks Register	A-24
Figure A-5.1-1. Managing Financial Resources	A-31
Figure A-5.2-1. AT&T Hiring Process	A-33
Figure A-6.1-1. [REDACTED]	A-38
Figure A-6.4-1. AT&T's Product and Service Assurance Team:	A-40
Figure A-7.1-1. [REDACTED]	A-42
Figure A-7.2.2-1. [REDACTED]	A-45
Figure A-7.2.2-2. [REDACTED]	A-45
Figure A-7.2.2-3. Subcontractor Strategic Sourcing Process	A-46
Figure A-7.2.2-4. [REDACTED]	A-47
Figure A-7.2.2-5. [REDACTED]	A-48
Figure A-7.2.2-6. [REDACTED]	A-51
Figure A-7.2.2-7. EIS Escalation Pathways	A-52
Figure A-8-1. [REDACTED]	A-54
Figure A-9.1-1. [REDACTED]	A-60
Figure A-9.1-2. AT&T's RMF Life Cycle	A-61
Figure B-1. AT&T Global Supply Chain Organization	B-2

Figure B-1-1. AT&T Supplier Portal.....	B-3
Figure B-1-2. Partner Evaluation Criteria.....	B-4
Figure B-1-3. AT&T Prospective Suppliers Website.....	B-4
Figure B-3-1. AT&T SCRM Overview.....	B-7
Figure B-4.4-1. AT&T Critical Analysis.....	B-16
Figure B-7-1. AT&T Risk Framework.....	B-22
Figure C-1. AT&T Portal and BSS.....	C-1
Figure C-2. BSS Verification Test Approach.....	C-3
Figure C-1-1. BSS Verification Test Plan Scope.....	C-3
Figure C-1-2. [REDACTED].....	C-4
Figure C-1.1-1. [REDACTED].....	C-5
Figure C-2.2-1. [REDACTED].....	C-10
Figure C-3.11-1. [REDACTED].....	C-32
Figure C-4-1. [REDACTED].....	C-34
Figure C-4.2-1. [REDACTED].....	C-35
Figure C-4.4-1. [REDACTED].....	C-35
Figure C-5.1-1. [REDACTED].....	C-36
Figure D-1. [REDACTED].....	D-1
Figure D-1.1-1. Service Test Plan Process Flow.....	D-5
Figure D-1.4-1. Service Test Plan Process Flow.....	D-12
Figure D-1.6-1. DFS Test Plan Process Flow.....	D-16
Figure F-1. [REDACTED].....	F-2
Figure F-2. [REDACTED].....	F-2
Figure G-4.2-1. [REDACTED].....	G-8
Figure G-4.19-1. [REDACTED].....	G-22
Figure H-1. National Disaster Recovery Team Equipment.....	H-6
Figure H-2. [REDACTED].....	H-10
Figure H-3.1-1: AT&T's Network Architecture.....	H-14
Figure H-3.1-2. [REDACTED].....	H-15
Figure H-3.1-3. [REDACTED].....	H-16
Figure H-3.1-4: GETS enabled IP Call Processing.....	H-18
Figure H-2. AT&T Worldwide Control Center.....	H-21

LIST OF TABLES

Table 1-1. Management and Functional Areas	2
Table 1.1-1. Management Approach Features and Benefits.....	7
Table 1.1.1-1. Ordering Approach and Capability.....	9
Table 1.1.1-2. Compliance with TO Process Requirements.....	11
Table 1.1.1-3. Ordering Notices.....	12
Table 1.1.1-4. General and Functional Ordering Requirements.....	14
Table 1.1.1-5. EIS Order Types.....	14
Table 1.1.1-6. TOPP Report Elements.....	18
Table 1.1.2-1. Features and Benefits for GSA.....	21
Table 1.1.2-2. Billing Processes, Data and System Interfaces.....	23
Table 1.1.2-3. Additional Billing Requirements.....	26
Table 1.1.3-1. AT&T Web-based Systems BSS Features and Benefits.....	30
Table 1.1.4-1. AT&T CSO.....	42
Table 1.1.5-1.	44
Table 1.1.5-2.	46
Table 1.1.6-1.	47
Table 1.1.6-2. SOCN Data Elements.....	50
Table 1.1.6-3.	52
Table 1.1.6-4.	54
Table 1.1.7-1.]	60
Table 1.1.7-2.	62
Table 1.1.7-3. Standard Service Provisioning Intervals [G.8.2.2.1.1].....	62
Table 1.1.7-4.	63
Table 1.1.7-5. Standard Service Provisioning Intervals [G.8.2.2.1.1].....	64
Table 1.1.7-6.	66
Table 1.1.8-1. AT&T's Training Curriculum.....	69
Table 2.1-1. AT&T's EIS Service and BSS Testing.....	71
Table 2.2.1-1. BSS Inspection and Acceptance.....	75
Table 2.2.1-2. Scenarios.....	76
Table 2.2.1-3. Test Environment and Conditions.....	76
Table 3.1-1. Secure, Efficient CDIP-Compliant Data Exchange.....	80
Table 3.2-1. Common Data Interaction Requirements.....	82
Table 3.3-1. Deliverables and Data Exchange.....	84
Table 3.4-1. CDIP Common Operational Requirements.....	84
Table 3.4-2. Order Types and Responses.....	86
Table 3.4-3. Ordering Deliverables and Data Exchange.....	87

Table 3.5-1. CDIP Billing.....	88
Table 3.5-2. Billing Process Deliverables.....	89
Table 3.5-3. Billing Process Deliverables and Data Exchange.....	90
Table 3.6-1. CDIP Disputes Requirements.....	91
Table 3.7-1. CDIP Inventory Requirements.....	92
Table 3.8-1. CDIP SLA Management Requirements.....	93
Table 3.9-1. Data Transfer Mechanisms.....	94
Table 3.10-1. CDIP Other Data Dictionary Requirements.....	95
Table 3.10-2. Order Types.....	96
Table 3.10-3. Data Set Structure.....	97
Table 3.10-4. Primary Data.....	98
Table 3.10-5. Reference Data.....	99
Table 3.10-6. Task Order Data.....	100
Table A-1. EIS PMP Summary.....	A-1
Table A-1-1. Assumptions and Dependencies.....	A-2
Table A-2.1-1. Compliance with Ordering Requirements.....	A-5
Table A-2.2-1. Compliance with Billing Requirements.....	A-6
Table A-2.3-1. [REDACTED].....	A-8
Table A-2.4-1. Compliance with Service Management Requirements.....	A-9
Table A-4.1-1. AT&T Transition Project Management Features and Benefits.....	A-17
Table A-4.1-2. AT&T's Transition Activities.....	A-18
Table A-4.1.1-1. Approach to Functional Processes.....	A-20
Table A-4.1.1-2. Examples of Transition Off Planning.....	A-21
Table A-4.1.2-1. Expediting Transition as the Incumbent.....	A-22
Table A-4.2-1. Quotations and Proposals.....	A-25
Table A-4.2.1-1. Approach to Assisting Agencies.....	A-25
Table A-4.4.3-1. Example Steps to Mitigate Possible Impact to Customers Operations.....	A-28
Table A-4.5-1. Transition Contingency Roles and Responsibilities.....	A-29
Table A-4.5-2. Processes for Contingency/Fall-Back.....	A-29
Table A-5.2-1. AT&T Comprehensive Employee Retention Programs.....	A-33
Table A-5.2-2. Methodologies for Effective Utilization of Personnel.....	A-34
Table A-6-1. [REDACTED].....	A-36
Table A-6-2. [REDACTED].....	A-37
Table A-6-3. [REDACTED].....	A-37
Table A-7-1. AT&T Key Personnel and Capabilities.....	A-41
Table A-7.2-1. [REDACTED].....	A-42

Table A-7.2.1-1. [REDACTED]	A-43
Table A-7.2.2-1. AT&T's Coordination and Communications.	A-48
Table A-7.2.2-2. [REDACTED]	A-51
Table A-8-1. [REDACTED]	A-54
Table A-8.1-1. The AT&T High-Level Process for EIS Program Risk Identification and Mitigation.	A-55
Table A-8.1-2. AT&T EIS Program Risk Management Team.	A-56
Table A-8.1-3. AT&T Analysis Process.	A-56
Table A-8.1-4. AT&T's Risk Mitigation Steps.	A-57
Table A-8.1-5. Potential EIS Program Risk.	A-58
Table B-1. AT&T SCRM Plan Benefits.	B-3
Table B-1-1. AT&T TL9000 Measurements Summary Listing.	B-5
Table B-3-1. AT&T Five Supply Chain Phases	B-7
Table B-4.3-1. NIST System Acquisition Controls from NIST Special Publication 800-53A.	B-13
Table C-2.2-1. BSS Verification Test.	C-10
Table C-3-1. [REDACTED]	C-13
Table C-3-2. [REDACTED]	C-14
Table C-3.1-1. Test Case for Direct Data Exchange – XML Over Secure Web Services.	C-15
Table C-3.1-2. Test Case for Direct Data Exchange – PSV Over SFTP.	C-15
Table C-3.1-3. Test Case for Direct Data Exchange – Error Handling.	C-15
Table C-3.1-4. Test Case for Direct Data Exchange – Error Handling.	C-16
Table C-3.2-1. Test Case for Task Order Data Management.	C-16
Table C-3.3-1. Test Case for Role Based Access Control.	C-17
Table C-3.3-2. Test Case for Role Based Access Control – Unauthorized User Access Denial Verification.	C-17
Table C-3.4-1. Test Case for Service Ordering – New Order via Web Interface.	C-18
Table C-3.4-2. Test Case for Service Ordering – New Order via Email.	C-18
Table C-3.4-3. Test Case for Service Ordering – Disconnect Order.	C-19
Table C-3.4-4. Test Case for Service Ordering – Feature Addition Order.	C-19
Table C-3.4-5. Test Case for Service Ordering – Move Order.	C-19
Table C-3.4-6. Test Case for Service Ordering – TSP Order.	C-20
Table C-3.4-7. Test Case for Service Ordering-Auto Sold CLINS.	C-21
Table C-3.4-8. Test Case for Service Ordering – Task Order Unique CLINS (TUCs).	C-21
Table C-3.4-9. Test Case for Service Ordering – Bulk Orders.	C-21

Table C-3.4-10. Test Case for Service Ordering – Error Checking, Missing Information.	C-22
Table C-3.4-11. Test Case for Service Ordering – Error Checking Invalid Info.	C-22
Table C-3.5-1. Test Case for Supplements to In-Progress Orders – Cancel Orders.	C-23
Table C-3.5-2. Test Case for Supplements to In Progress Orders – Service Feature Change	C-23
Table C-3.5-3. Test Case for Supplements to in Progress Orders Location Change.	C-24
Table C-3.5-4. Test Case for Supplements to In Progress Orders – Change to Customer Want Date.	C-25
Table C-3.5-5. Test Case for Supplements to In Progress Orders – Change to Administrative Data.	C-25
Table C-3.6-1. Test Case for Administrative Change Order – Administrative Change Order.	C-26
Table C-3.7-1. Rapid Provisioning & Self-Provisioning Orders – Rapid Provisioning Orders.	C-26
Table C-3.7-2. Rapid Provisioning and Self-Provisioning Orders – Self-Provisioning Orders.	C-27
Table C-3.7-3. Rapid Provisioning & Self-Provisioning Orders – Self-Provisioning Orders: Error Checking.	C-27
Table C-3.8-1. Inventory and Billing – Self-Provisioning Orders – Inventory Reconciliation.	C-28
Table C-3.8-2. Inventory and Billing – Self-Provisioning Orders – Billing.	C-28
Table C-3.8-3. Inventory and Billing – Self-Provisioning Orders – Usage Based Billing.	C-29
Table C-3.8-4. Inventory and Billing – Self-Provisioning Orders – Billing Adjustments.	C-29
Table C-3.9-1. Dispute Handling – Self-Provisioning Orders – Government Initiated Dispute.	C-30
Table C-3.10-1. SLA Management – SLA Reporting.	C-31
Table C-3.10-2. SLA Management – SLA Credit Request.	C-31
Table C-3.11-1. Open-Format Reporting – Open-Format Reporting: Samples.	C-31
Table C-3.12-1. Test Case for Regression Testing.	C-32
Table C-3.13-1. Test Case for Security Testing.	C-32
Table C-4-1. Testing Details.	C-33
Table D-1.1-1. EIS Virtual Private Network Service Test Plan.	D-4
Table D-1.1-2. VPNS Verification Test Plan Locations and Port Speeds.	D-5
Table D-1.1-3. Service-Specific Verification Test Cases. [C.2.1.1.4]	D-6
Table D-1.2-1. Ethernet Transport Service Verification Test Plan.	D-7
Table D-1.2-2. Ethernet Transport Service Locations and Speeds.	D-7
Table D-1.2-3. Service Specific Verification Test Cases. [C.2.1.2.4]	D-8

Table D-1.3-1. Optical Wavelength Service Verification Test Plan.....	D-9
Table D-1.3-2. Optical Wavelength Service Parameters.....	D-9
Table D-1.3-3. Test Cases [C.2.1.3.4].....	D-10
Table D-1.4-1. Private Line Service Verification Test Plan.....	D-11
Table D-1.4-2. Private Line Service Test Cases. [C.2.1.4.4].....	D-12
Table D-1.5-1. Synchronous Optical Network Service Verification Test Plan.....	D-14
Table D-1.5-2. SONET Port Speeds.....	D-14
Table D-1.5-3. Synchronous Optical Network Test Cases. [C.2.1.5.4].....	D-15
Table D-1.6-1. Dark Fiber Service Verification Test Plan.....	D-16
Table D-1.6-2. Dark Fiber Service Verification Test Cases. [C.2.6.1.4].....	D-17
Table D-1.7-1. Internet Protocol Service Verification Test Plan.....	D-18
Table D-1.7-2. IPS Port Speeds.....	D-19
Table D-1.7-3. IPS Verification Test Cases.....	D-20
Table D-1.8-1. [REDACTED].....	D-20
Table D-2.1-1. Internet Protocol Voice Service Verification Test Plan.....	D-23
Table D-2.1-2. IPVS Access Speeds.....	D-23
Table D-2.1-3. IPVS Verification Test Cases.....	D-24
Table D-2.2-1. [REDACTED].....	D-25
Table D-2.2-2. [REDACTED].....	D-26
Table D-2.3-1. Toll Free Service Verification Test Plan.....	D-27
Table D-2.3-2. Toll Free Service Verification Test Cases.....	D-28
Table D-2.4-1. [REDACTED].....	29
Table D-2.4-2. [REDACTED].....	D-30
Table D-3.1-1. Contact Center Service.....	D-31
Table D-4.1-1. Collocated Hosting Service Verification Test Plan.....	D-32
Table D-5.1-1. [REDACTED].....	D-33
Table D-5.2-1. [REDACTED].....	D-34
Table D-5.3-1. [REDACTED].....	D-36
Table D-5.4-1. Content Delivery Verification Test Plan.....	D-37
Table D-6.1-1. Wireless Service Verification Test Plan.....	D-39
Table D-7.1-1. [REDACTED].....	D-40
Table D-7.1-2. CSCS Interface Port Speeds.....	D-41
Table D-7.2-1. [REDACTED].....	D-42
Table D-7.2-2. [REDACTED].....	D-43
Table D-8.1-1. Managed Network Service Verification Test Plan.....	D-44
Table D-8.1-2. Managed Network Service Access Speed.....	D-44
Table D-8.2-1. Web Conferencing Service Verification Test Plan.....	D-45
Table D-8.3-1. Unified Communications Service Verification Test Plan.....	D-46

Table D-8.3-2. Unified Communications Service Network Access Speed.....	D-47
Table D-8.3-3. UCS Verification Test Cases.	D-48
Table D-8.4-1. Trusted Internet Protocol Service Verification Test Plan.	D-48
Table D-8.4-2. MTIPS Port Speeds.....	D-48
Table D-8.4-3. MTIPS KPI Parameters to be Measured.	D-50
Table D-8.4-4. MTIPS KPI Verification Test Cases. [C.2.8.4.4]	D-51
Table D-8.5-1. Managed Security Service Verification Test Plan.....	D-52
Table D-8.5-2. [REDACTED]	D-52
Table D-8.5-3. [REDACTED]	D-54
Table D-8.6-1. Managed Mobility Service Verification Test Plan.....	D-55
Table D-8.6-2. [REDACTED]	D-57
Table D-8.7-1. Table Audio Conferencing Service Verification Test Plan.	D-58
Table D-8.7-2. ACS Verification Test Cases.	D-59
Table D-8.8-1. [REDACTED]	D-59
Table D-8.8-2. [REDACTED]	D-61
Table D-8.9-1. DHS Intrusion Detection Service Verification Test Plan.	D-61
Table D-8.10-1. [REDACTED]	D-63
Table E-2-1. AT&T Leadership in Sustainability.....	E-9
Table E-2-2. AT&T Leading Sustainability Through Action.	E-11
Table G-4.1-1. Sample BSS Hardware/Software Matrix.....	G-7
Table G-4.4-1. Sample Control Summary Table.	G-9
Table G-4.24-1. NIST SP Policies.	G-26
Table G-5.1-1. BSS Deliverables.	G-28
Table H-1. AT&T NS/EP Approach and Capabilities.	H-2
Table H-2. AT&T Number Translation Service.	H-5
Table I-1-1. [REDACTED]	I-1

ABBREVIATION AND ACRONYM DEFINITION LIST

Abbreviation/Acronym	Definition
A&A	Assessment and Authorization
AB	Agency Bureau
ABCODE	Agency Bureau Code
AC	Assessment Control
ACO	Administrative Change Orders
ACS	Audio Conferencing Service
ACT/IAC	American Council for Technology/Industry Advisory Council
ACTINA	Active/Inactive
ACTTYP	Account Type
ADJOUT	Adjustment Outcome
ADJRSN	Adjustment Reason
AFRAM	Access Framing
AFU	Approved for Use
AFV	Alternative Fuel Vehicles
AGF	Associated Government Fee
AGFD	Associated Government Fee Detail
AHC	Agency Hierarchy Code
AIA	Application Impact Analysis
ALLTAX	Allowable Tax
AMP	Accessibility Management Platform
ANSI	American National Standards Institute
ANSI/EIA-748	American National Standards Institute/Electronic Industries Alliance
AO	Authorizing Official
API	Application Program Interface
APROV	Access Provisioning
AQL	Acceptable Quality Level
ASCP	Advanced Supply Chain Planning
ASN	AT&T Switched Network
ASPR	AT&T Security Policy and Requirements
ASRN	Agency Service Request Number
AT&T	American Telephone & Telegraph
ATIS	Alliance for Telecommunications Industry Solutions
ATO	Authority to Operate
ATQ	Authority to Quote
ATR	AGF Electronic Funds Transfer
Av	Availability
BA	Billing Adjustment
BANDW	Bandwidth
BCI	Bit Count Integrity
BCP	Business Continuity Plan
BD	Billing Detail
BERT	Bit Error Rate Test
BI	Billing Invoice
BIA	Business Impact Assessment

Abbreviation/Acronym	Definition
BLOB	Binary Large Object
BSD	Boundary Scope Document
BSS	Business Support System
BSS	Business Support Systems
C&S	Citizenship Sustainability
CA	Criticality Analysis
CATO	Corporate Accessibility Technology Office
CBSA	Core Based Statistical Area
CC	Control Center
CCRR	Customer Complaint Report Rate
CCS	Contact Center Service
CD	Chromatic Dispersion
CDI	Common Data Interaction
CDIP	Contract Data Interaction Plan
CDIP	Contractor Data Interaction Plan
CDNS	Content Delivery Network Service
CDP	Carbon Disclosure Project
CDRL	Contract Data Requirements List
CE	Client Executives
CEO	Chief Executive Officer
CFA	Circuit Facility Availability
CFR	Code of Federal Regulations
CIA	Continuous Integration Automation
CIM	Customer Information Management
CIO	Chief Information Officer
CIO-IT	Chief Information Officer – Information Technology
CIS	Center for Internet Security
CKTTYP	Circuit Type
CLIN	Contract Line Item Number
CLINs	Contract Line Item Numbers
CLONES	Central Location Online Entry System
CM	Configuration Management
CMMI	Capability Maturity Model Integration
CMP	Configuration Management Plan
CNSSI	Committee or National Security Systems Instruction
CNTRY	Country
CO	Contracting Officer
CO2	Carbon Dioxide
COE	Center of Excellence
COLT	Cell on Light Truck
CONUS	Continental United States
COO	Chief Operations Officer
COOP	Continuity of Operations Plan
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative

Abbreviation/Acronym	Definition
COTS	Commercial Off the Shelf
COW	Cells on Wheels
CP	Contingency Plan
CPC	Calling Party's Category
CPCS	Call Processing Control System
CPE	Customer Premise Equipment
CPM	Communications Portfolio Management
CPM	Communications Portfolio Management
CPTP	Contingency Plan Test Plan
CRGFRQ	Charging Frequency
CRGUNT	Charging Unit
CSA	Customer Service Authorization
CSCS	Commercial Satellite Communications Service
CSO	Customer Service Office
CSO and GP	Chief Strategy Officer and Group President
CSR	Customer Service Representatives
CSRN	Contractor Service Request Number
CSU/DSU	Channel Service Unit/Data Service Unit
CSV	Comma-Separated Values
CTO	Chief Technology Office
CUI	Controlled Unclassified Information
CWD	Customer Want Date
DB	Database
DBA	Direct-Billed Agency
DBAS	Direct-Billed Agency Setup
DESSC	Digital Energy Sustainability Solutions Campaign
DFS	Dark Fiber Service
DHS	Dedicated Hosting Service
DHS	Department of Homeland Security
DM	Degraded Minutes
DMS-250	Digital Multiplex System Model 250
DNS	Domain
DOE	Department of Energy
DoJ	Department of Justice
DPA	Delegation of Procurement Authority
DPA	Delegations of Procurement Authority
DR	Dispute Report
DRP	Disaster Recovery Plan
DRSN	Dispute Reason
DS1	Digital Signal 1
DS2	Digital Service 2
DS3	Digital Service 3
DSTUS	Dispute Status
DTT	Data Transaction Type

Abbreviation/Acronym	Definition
E2E	End to End
EDC	Emergency Communications Division
ECOS	End-to-End Class of Service
ECV	Emergency Communications Vehicles
EDF	Environmental Defense Fund
EFS	Error Free Seconds
EFT	Electronic Funds Transfer
EIS	Enterprise Infrastructure Solution
EIT	Electronic Information Technology
eMLPP	enhanced Multi-Level Precedence and Pre-emption
EN	Event Notification
eNPS	Employee Net Promoter Score
EO	Executive Order
EOP	Executive Office of the President
EP	Emergency Preparedness
EPA	Environmental Protection Agency
EPEAT	Electronic Product Environmental Assessment Tool
ERG	Employee Resource Groups
ES	Errored Seconds
ETS	Ethernet Transport Service
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FASTAR	Fast Automatic Restoration
FCC	Federal Communications Commission
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
FEMP	Federal Energy Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOC	Firm Order Commitment
FOCN	Firm Order Commitment Notice
FOIA	Freedom of Information Act
FSO	Facilities Security Office
FTP	File Transfer Protocol
FTP	File Transport Protocol
FY	Fiscal Year
FY16	Fiscal Year 2016
GAO	Government Accountability Office
GEMI	Global Environmental Management Initiative
GETS	Government Emergency Telecommunications Service
GETS	Government Emergency Telecommunications Service
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GHG	Greenhouse Gas
GMP	Government Markets Platform
GOS	Grade of Service
GPM	Global Project Managers

Abbreviation/Acronym	Definition
GPS	Global Positioning System
GRI	Global Reporting Initiative
GSA	General Services Administration
GSAM	General Services Administration Acquisition Manual
GSC	Global Supply Chain
GSM	Global System for Mobile
GSS	Global Support System
HECI	Human Equipment Category Inventory
HPC	High Probability of Completion
HR	Human Resources
HSPD	Homeland Security Presidential Directive
HSPD-12	Homeland Security Presidential Directive-12
HTML	HyperText Markup Language
HTTPS	Hypertext Transfer Protocol Secure
HUBZone	Historically Underutilized Business Zones
HVAC	Heating, Ventilating, and Air Conditioning
HW	Hardware
I&A	Identification and Authentication
I&T	Integration and Testing
IA	Interagency Agreement
IAC	Industry Advisory Council
IAM	Initial Address Message
IAW	In accordance with
ICB	Individual Case Basis
ICB	Individual Case Basis
ICBS	Individual Case Basis(s)
ICT	Information and Communications Technology
ID	Identification or Identifier
IDP	Individual Development Plan
IDP	Intrusion Detection and Prevention
IDPS	Intrusion Detection and Prevention Service
IDS	Intrusion Detection Systems
IMS	Integrated Master Schedule
INRS	Incident Response Service
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPS	Internet Protocol Service
IP-VPN	Internet Protocol – Virtual Private Network
IPVS	Internet Protocol Voice Service
IR	Inventory Reconciliation
IR	Inventory Reconciliation
IR	Incident Response
IRP	Incident Response Plan
IRS	Internal Revenue Service
IRTR	Incident Response Test Report
ISA	Interconnection Security Agreements

Abbreviation/Acronym	Definition
ISCM	Information Security Continuous Monitoring
ISO	International Organization for Standardization
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITIL	IT Infrastructure Library
ITT	Information Technology Tools
ITU	International Telecommunication Union
ITU-TSS	International Telecommunications Union – Telecommunication Standardization Sector
IXC	Inter-exchange Carrier
JAWS	Job Access With Speech
JCKTYP	Jack Type
JUTNet	Justice Unified Telecommunications Network
KPI	Key Performance Indicator
KPIAO	KPI AQL Type
KPILQ	KPI Location Qualifier
KPIMU	KPI Measurement Unit
KPISLQ	KPI Service Level Qualifier
KPIUC	KPI Unit Code
LEC	Local Exchange Carrier
LGC	Local Government Contact
LNECD	Line Coding
LNP	Local Number Portability
LOA	Letter of Authorization
LOADEP	LOA Dependencies
LOF	Loss of Frame
Los	Loss of Signal
LSA	Local Service Agreement
LTE	Long-Term Evolution
MACD	Moves Adds Changes and Disconnects
MCB	Management Control Bridge
MMF	Multi-Mode optical Fiber
MMS	Managed Mobility Service
MOA	Memorandum of Agreement
MOS	Mean Opinion Score
MOU	Memorandum of Understanding
MP	Media Protection
MPLS	Multi-Protocol Label Switching
MPS	Managed Prevention Service
MRC	Monthly Recurring Charges
MSC	Mobile Switching Center
MSOC	Management System and Operating Control
MSS	Managed Security Service
MTIPS	Managed Trusted Internet Protocol Service
MTP	Message Transfer Part
MTTLBCI	Mean Time to Loss of BCI
MWS	Wireless Service

Abbreviation/Acronym	Definition
N/A	Not Applicable
NASCAR	National Association for Stock Car Auto Racing
NB-IPVPN	Network Based — Internet Protocol Virtual Private Network
NCS	National Communications System
NCSD	NCS Directive
NDA	Nondisclosure Agreements
NDR	Network Disaster Recovery
NEBS	Network Equipment-Building System
NGA	Non-Governmental Agencies
NGN	Next Generation Network
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NIST.SP	National Institute of Standards and Technology Special Publication
NLT	No Later Than
NLT	No Later Than
NMC	Network Management Controls
NOC	Network Operations Center
NPA	Numbering Plan Area
NPR	Number of Problem Reports
NRC	Non-Recurring Charges
NS	National Security
NS/EP	National Security and Emergency Preparedness
NS/EP	National Security and Emergency Preparedness
NS2020	Network Services 2020
NSA	National Security Agency
NSA	National Security Agency
NSC	Network Site Code
NSDD	National Security Decision Directive
NSSE	National Special Security Events
NT	Number Translation
NTP	Network Time Protocol
NTP	Notice to Proceed
O&M	Operations and Maintenance
OC-12	Optical Carrier 12
OC-192	Optical Carrier 192
OC3	Optical Carrier 3
OC-48	Optical Carrier 48
OCO	Ordering Contracting Officer
OCONUS	Outside Contiguous United States
OEC	Office of Emergency Communications
OEC	Office of Emergency Communications
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OP123	Operating Practice No. 123
OP6	Operating Practice No. 6
OPT	Office of Priority Telecommunications
ORA	Order Receipt Acknowledgement

Abbreviation/Acronym	Definition
ORDHRD	Order Type: Header Level
ORDITM	Order Type: Line Item Level
ORDREJ	Order Rejection
OSAISO	Office of the Senior Agency Information Security Officer
OSS	Operations Support Systems
OSTP	Office of Science and Technology Policy
OTD	On-Time Delivery
OTDR	Optical Time-Domain Reflectometer
OWS	Optical Wavelength Service
PAO	Product Assurance Organization
PC	Personal Computer
PDF	Portable Document Format
PDF/CSV	Portable Document Format/Comma-Separated Value
PDN	Pseudo Destination Number
PE	Physical and Environment
PEA	Product Evaluation Agreements
PIA	Privacy Impact Assessment
PIC	Presubscribed Interexchange Carrier
PIC	Primary Interchange Carrier
PIC/LPIC	Presubscribed Interexchange Carrier/Local Prescribed Interexchange Carrier
PII	Personally Identifiable Information
PIID	Procurement Instrument Identifier
PIN	Personal Identification Number
PIP	Personal Integrity Plan
PL	Planning
PL	Public Law
PLS	Private Line Service
PM	Program Manager
PMBOK	Project Management Body of Knowledge
PMD	Polarization Mode Dispersion
PMI	Project Management Institute
PMO	Program Management Offices
PMP	Program Management Plan
POA&M	Plan of Action and Milestones
POC	Point of Contact
POP	Point of Presence
POTS	Plain Old Telephone Service
PPD	Presidential Policy Directive
PS	Personnel Security
PS	Priority Services
PS-Prep	Private Sector Preparedness Program
PSTN	Public Switched Telephone Network
PSV	Pipe Separated Value
PTA	Privacy Threshold Analysis
PTS	Priority Telecommunications Services
PUE	Power Utilization Efficiencies

Abbreviation/Acronym	Definition
QA	Quality Assurance
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QMS	Quality Management System
QoS	Quality of Service
R&D	Research and Development
RAPID	Restoration and Provisioning Integrated Design
RBAC	Role Based Access Control
RCA	Root Cause Analysis
REA	Rural Electrification Agency
RFP	Request for Proposal
RFQ	Request for Quote
RFQ/RFP	Request for Quotation/Request for Proposal
RIM	Record and Information Management
RMF	Risk Management Framework
RMP	Risk Managers Program
RoB	Rules of Behavior
RRAP	Repetitive Routing Attempt Procedure
RT	Recovery Type
RTNR	Real Time Network Routing
RTO	Recovery Time Objective
SA	Services Acquisition
SA	System Acquisition
SAP	Security Assessment Plan
SAR	Security Assessment Report
SAR	Search and Rescue
SATCOM	Satellite Communications
SC	System and Communication
SCIF	Sensitive and Classified Information Facilities
SCRM	Supply Chain Risk Management
SDN	Software Defined Networking
SDP	Service Delivery Point
SED	Service Enabling Devices
SES	Severely Errored Seconds
SFTP	Secure File Transport Protocol
SI	System and Information
SISR	Supplier Information Security Requirements
SLA	Service Level Agreement
SLACR	SLA Credit Report
SLACR	SLA Credit Request
SLAR	Service Level Agreement Report
SME	Subject Matter Experts
SMF	Single Mode optical Fiber
SO	Service Order
SOA	Service Order Acknowledgement

Abbreviation/Acronym	Definition
SOAC	Service Order Administrative Change
SOAP	Simple Object Access Protocol
SOC	Service Order Confirmation
SOCN	Service Order Completion Notice
SONET	Synchronous Optical Network
SONETS	Synchronous Optical Network Service
SORN	Service Order Rejection Notice
SORN	System of Records Notice
SOW	Statement of Work
SP	Special Publication
SP	Special Publication
SPR	Software Problem Report
SQL	Structured Query Language
SRE	Service Related Equipment
SS7	Signaling System 7
SSB	SSB Bart Group
SSCN	Service State Change Notice
SSH	Secure Shell
SSP	System Security Plan
SVC	Service
SVN	Subversion
SW	Software
TAX	Tax Detail
TBD	To Be Determined
TCB	Technical Control Bridge
TCP	Transmission Control Protocol
TDD	Telecommunications Device for the Deaf
TDM	Time Division Multiplexing
TE	Traffic Engineering
TEER	Telecommunications Energy Efficiency Ratio
TFS	Toll Free Service
TIC	Trusted Internet Connection
TL	Telecom Leadership
TL9000	Telecom Leader 9000
TMP	Transition Management Plans
TO	Task Order
TOPP	Task Order Project Plan
TP&E	Technology Planning & Engineering
TPAP	Third Party Assessment Process
TPD	Technical Provisioning Document
TRUFLS	True/False
TS	Test Scenario
TS/SCI	Top Secret/Sensitive Compartmented Information
TS-01	Test Scenario 1
TS-02	Test Scenario 2
TS-03	Test Scenario 3
TSMP	Transition Strategy and Management Plan

Abbreviation/Acronym	Definition
TSN	Trusted Systems and Networks
TSNOW	Transport Service Now
TSP	Telecommunication Service Priority
TSR	Telecommunications Service Request
TTR	Time to Restore
TUC	TO Unique CLIN
UAT	User Acceptance Testing
UBI	Unique Billing Identifiers
UC	Unified Communications
UCS	Unified Communications Service
UCT	User Certification Test
UMTS	Universal Mobile Telecommunications System
VIP	Velocity IP
VoIP	Voice over Internet Protocol
VPAT	Voluntary Product Accessibility Template
VPN	Virtual Private Network
VPNS	VPN Service
VPNS	Virtual Private Network Service
VSS	Vulnerability Scanning Service
VT	Virtual Tributary
WBS	Work Breakdown Structure
WCAG	Web Content Accessibility Guidelines
WCS	Web Conferencing Service
WDM	Wavelength Division Multiplexing
WiFi	Wireless Fidelity
WO	Warehouse Operations
WPS	Wireless Priority Service
WSDL	Web Services Definition Language
XML	Extensible Markup Language
XSD	Extensible Markup Language Schema Definitions
YESNO	Yes No

VOLUME 2 — MANAGEMENT [L.30; L.11; L.9; M.2(2); M.2.2; G; E; J.2; C.3; D; F; H.10; H.35]

1 Management Response to Requirements for Section G: Contract Administration Data [L.30(1); L.30.1(1); M.2(2); M.2.2; G; G.1]

General Services Administration (GSA) and customer agencies will receive an in-place Customer Support Office (CSO) tailored for Enterprise Infrastructure Solution (EIS), a highly secure portal and enhanced suite of business support systems that exceeds the minimum requirements, with Networkx-proven experienced leadership. Combined, the aforementioned offer continuity of service, deliver a smooth transition to EIS, provide the operational knowledge to systematically reduce program risk, and establish a platform for growth for the life cycle of EIS.

For GSA to become the strategic sourcing center for network-based and network-enabled Information Technology (IT) services, three integrated and equally critical management components within EIS are required:

1. An in-place CSO infrastructure that enables operational success
2. A highly secure portal and BSS that facilitate agency usage, and
3. Program understanding and leadership that delivers continuity of knowledge



Figure 1-1. Elements for Success. AT&T's management foundation directly supports GSA's vision for EIS.

AT&T has all three! These components, shown in **Figure 1-1**, form the basis required to successfully evolve beyond Networkx and regional Local Service Areas (LSA) by delivering a framework that achieves continuity of service while migrating to the EIS contract. **Section 1.1**, below, summarizes our core elements for success while identifying the GSA and agency benefits derived from our collective management offering. Throughout each section of this volume, AT&T provides our approach to the people, processes, and tools that will support and complement this base and, in turn,

directly support EIS to the benefit of the government. In detailing these strengths, our proposal follows the response outline of Request for Proposal (RFP) Section L.30, which aligns with the structure of RFP Section G, the contents of RFP Section E, and requirements of RFP Section J.2. To supplement this volume, we provide eight appendices to accurately comply with RFP Section L.30.2.

This volume describes how AT&T will support GSA and agencies by providing the domain knowledge and systems defined in RFP Section G.1 as indicated in **Table 1-1**. This table provides a cross reference to where we discuss our proposed management approach to these functional areas.

Table 1-1. Management and Functional Areas. *Our proposal covers all the management and functional areas specified in RFP paragraph G.1.*

Functional Area	Location in Volume 2
Contract Administration	Appendix A
Ordering	Section 1.1.1, Appendix A
Billing	Section 1.1.2, Appendix A
Business Support Systems	Section 1.1.3, Appendix A, Appendix C, Appendix G
Service Assurance	Section 1.1.4, Appendix A
Inventory Management	Section 1.1.6, Appendix A
Service Level Management	Section 1.1.7, Appendix A
Program Management	Appendix A
Training	Section 1.1.8
National Security and Emergency Preparedness	Appendix H
Requirements for Climate Change Adaptation, Sustainability and Green Initiatives	Appendix E
RFP Section J.2, Contractor Data Interaction Plan	Section 3

AT&T is compliant with all management requirements in the RFP. Program Management [G.9] and program management functions [G.9.1] are addressed in **Appendix A**. Performance measurement and contract compliance [G.9.2] is addressed in **sections 1.1.5, 1.1.7, and A.6 in Appendix A**. Coordination and Communication [G.9.3] is an integral part of our methodology and is discussed throughout this volume and more specifically in **A.7.2.2.4 in Appendix A**.

1.1 AT&T's Approach and Capability to Provide User-Friendly, Compliant and Efficient Support Systems [L.30.1(1)(a); M.2.2(1 of 3); G]

User-friendly, compliant, and efficient support systems require a combination of people, processes, and tools to deliver an effortless experience end-to-end. Accordingly, the AT&T approach combines a CSO team, which offers over eight consecutive years of program understanding from Networx and nearly 20 years regional Local Service

Agreements (LSA) experience to apply to EIS; processes enhanced from Networkx to provide EIS-compliant execution; and systems designed to EIS specifications, including

ease of customer use. Our CSO will integrate this know-how into a smooth, cohesive, and fully responsive customer experience.



Our Customer Support Office (CSO) Infrastructure: Managed under the direction of AT&T's EIS Program Manager (PM), our CSO directly supports GSA, sets direction for the support of agency customers, and serves to enable our overall operational success. The CSO coordinates and provides oversight of EIS task order (TO) execution performed by customer-aligned AT&T

service delivery teams and service providers. The AT&T Networkx CSO, located in AT&T facilities, is staffed today and will be available to fully support the EIS contract on day one of award.

AT&T supports a user-friendly, coordinated government customer experience with open and active communication paths as depicted by the orange arrowed lines in

Figure 1.1-1. The AT&T CSO acts as advisor and conduit for communications amongst all parties to enable effective contract execution and management. These communication channels are augmented by AT&T's existing relationships and engagements with the GSA and the agencies.

Agency-focused Client Executives (CE), shown in the top right of our figure, collaborate with agencies to understand unique requirements and provide assistance to validate the best solution to meet their immediate needs and evolving missions.

Contained on the bottom half of the figure are the functional groups comprising the CSO who focus on the daily management of the contract. Leading each of those groups are AT&T employees whose experience and subject matter specialists are directly commensurate with the scale, scope, and responsibilities for the EIS contract. This CSO leadership team has in-depth functional experience gained from providing similar services to GSA, over [REDACTED] agencies, and [REDACTED] subagencies under the current Networkx contract vehicles. These functional specialists will work collaboratively to provide agency customers and the GSA an effective, responsive, and user-friendly EIS

experience. That experience, initiated through our CSO structure and personnel is promoted through the use of our portal and BSS.

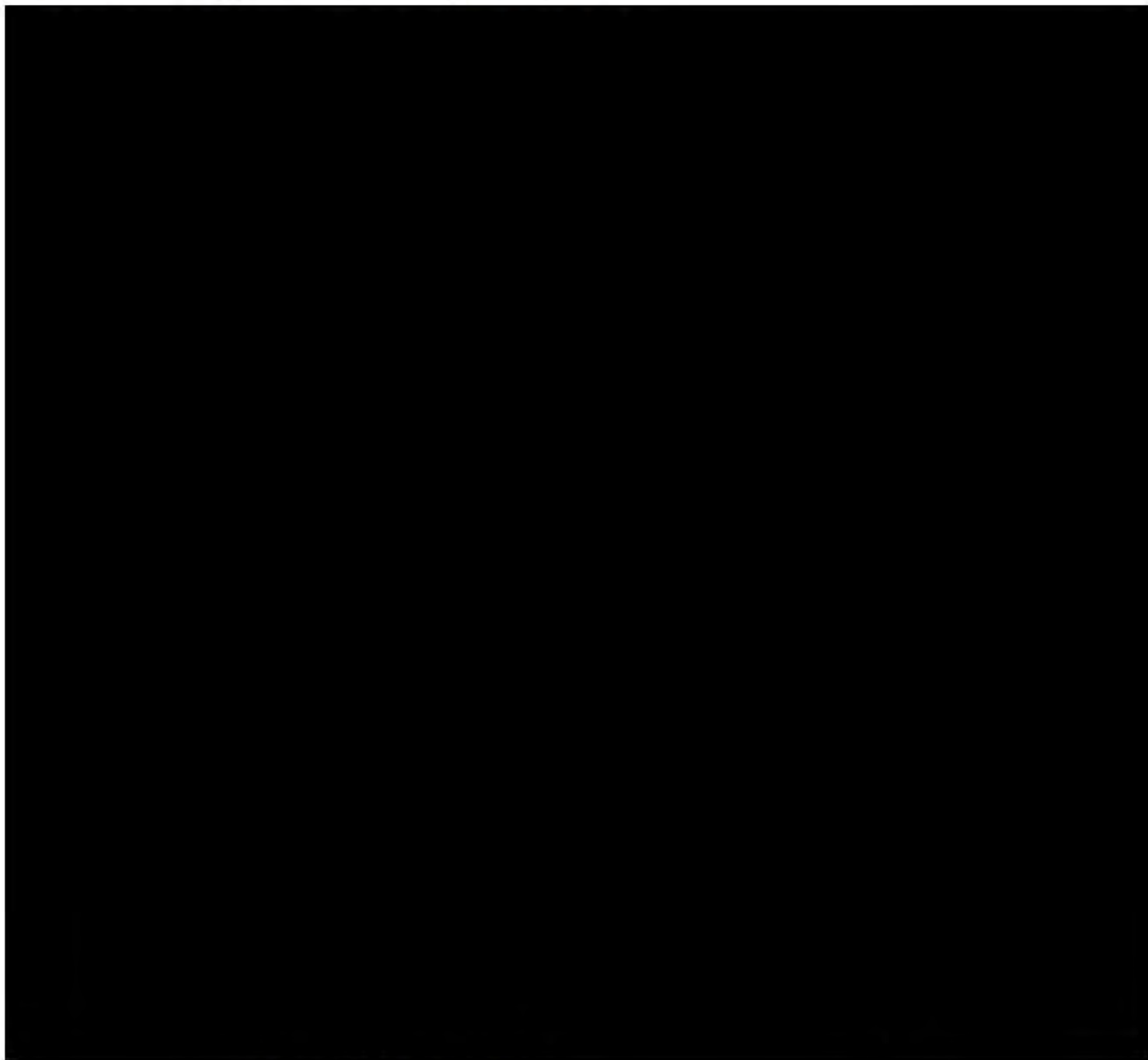
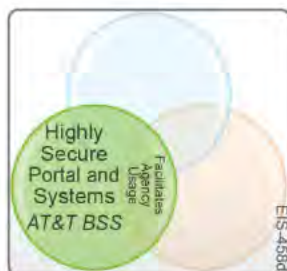


Figure 1.1-1. AT&T EIS CSO.



Our Highly Secure Portal and Business Support Systems (BSS): AT&T facilitates agency usage and supports data exchange communications via our BSS. This includes data exchanges with GSA Conexus as well as our Business Center web portal. Designed with the end-user in mind our portal, shown

in **Figure 1.1-2**, provides customer access to Government Center portal (shown in green), which is being enhanced to support the unique data and reporting requirements of EIS. AT&T Business Center web portal is the primary interface for EIS services and the AT&T BSS. AT&T uses two-factor authentication and role-based access to provide security for the BSS.



Figure 1.1-2. AT&T Portal and BSS.

AT&T's BSS efficiently collects, stores, and disseminates order and service data points throughout the contract life cycle. Designed to achieve transparency and connectivity to both GSA and the agencies is a compliant Contractor Data Interchange Plan (CDIP) compatible with GSA's Conexus system. **Figure 1.1-3** details this high-level interface.

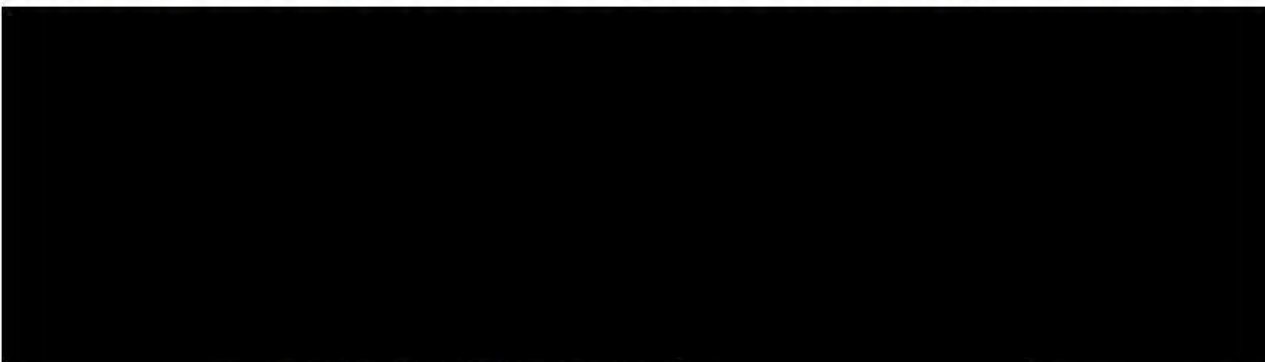


Figure 1.1-3. AT&T's High-Level CDIP.

The AT&T in-place CSO infrastructure, coupled with our highly secure web portal and BSS provides a structure and design that is both customer focused and user friendly. To deliver to GSA and the agencies the means to optimize these features and to implement the Network Services 2020 (NS2020) vision by successfully migrating to EIS requires a continuity of program understanding and the leadership to coalesce these elements into strengths.



Program Understanding and Leadership: The third component of our approach provides the GSA and agencies the understanding necessary to create a smooth pathway from Networkx, LSAs, and other contracts to EIS. [REDACTED], leads this compilation of knowledge, spread across our CSO. It is

[REDACTED] GSA program knowledge, understanding of agency and stakeholder needs and continual focus on customer satisfaction that will serve as the glue to merge our operational understanding together with GSA's vision for EIS. This continuity of knowledge, delineated in **Figure 1.1-4**, is the fundamental difference between merely providing a corporate offer to support EIS and having the corporate and customer knowledge to successfully achieve its goals.



Figure 1.1-4. AT&T's Continuity of Knowledge. [REDACTED]

Summary: The AT&T approach of providing an in-place CSO infrastructure, enhanced and highly secure BSS, and a corporate repository of program knowledge are integrated into all aspects of our EIS management approach. Combined with our commitment to customer satisfaction, it is emblematic of the business model that led AT&T to be named Fortune magazine's number one telecommunications company in 2015.

Table 1.1-1 highlights various features of our management approach that comprise and complement our elements for success. By providing these strengths and benefits, AT&T will assist GSA and customer agencies in meeting the EIS objectives of today and achieving the NS2020 vision for the future. Please note, that due to the interdependencies of support to be provided on EIS, columns 3 and 4 of **Table 1.1-1** pertain collectively to the individual items in columns 1 and 2.

Table 1.1-1. Management Approach Features and Benefits. GSA and agencies receive combined benefits from AT&T strengths that deliver the quality of systems, customer access, and ability to successfully migrate to EIS.

EIS Functions	Quality of Systems M.2.2(1)	Customer Access M.2.2(2)	Ability M.2.2(3)	Network Proof
Ordering	- Online access to submit and track orders - Dedicated order support team	Availability of all EIS tools to agencies via a single web portal with dual factor authentication. Includes role-based access controls (RBAC), which eliminates multiple log-ins and the need to save multiple links and juggle multiple rule sets	- GSA receives continuity of program knowledge dispersed throughout our CSO - CSO Staff provides 8 consecutive years of Network lessons learned that migrate to EIS	
Billing	- Accurate, timely invoices - Enhanced web tools to facilitate agency view and analysis of invoices and disputes - Experienced post-billing support team		- Risk managers employ process that has evolved through multiple GSA-like programs to mitigate performance risks - Transition managers have experience with agency-specific configurations and client executives' teams to expedite transition	Achieved contract-to-date invoice accuracy of
Business Support Systems	- Enhanced to increase functionality from Network - Designed to achieve transparency and connectivity to CDIP		Dedicated Client Executive teams focus on specific agencies, needs, and issues	
Customer Support Office and Technical Support	- Broad set of CSO and AT&T corporate resources to support agency transitions and life cycle needs - Dedicated contract modification team to adapt quickly to customer-specific needs and to keep EIS fresh with new and	Synergy between (1) the customer service provided within our CSO and EIS functions they support, (2) the quality of systems built into our design, and (3) the ease of use the GSA and Agency's receive	- Quality Management. - Established best practices includes International	- Supports agencies and subagencies - Successfully processed more than modifications in support of the GSA and

EIS Functions	Quality of Systems M.2.2(1)	Customer Access M.2.2(2)	Ability M.2.2(3)	Network Proof
	- expanded service capabilities - Dedicated, experienced CSO team - Multiple access points into the CSO: 844-EIS-ATT1, www.att.com/gov/eis	- Facilitates not discourages agency usage - Simplicity of access minimizes training requirements - Access design whose technology accommodates expansion throughout the period of performance	- Organization for Standardization (ISO), Project Management Body of Knowledge (PMBOK), IT Infrastructure Library (ITIL) standards - Transparent and fully compatible interface and formats to GSA Systems and Conexus	- agencies on the Network contracts - Has collaborated with GSA and agencies
Trouble Ticket Management	- Online ticketing for ease of initiating and tracking trouble reporting - Dedicated Tier 1 team to provide efficient, effective trouble handling			Transparent trouble ticket work tickets per quarter
Inventory Management	Enhanced web tools to facilitate agency view and analysis of inventory			Maintained over 500,000 items
Service Level Management	- Compliant reporting, visible via the web portal - Visibility into credit request process via online dispute tool			Submits compliant Service Level Agreement (SLA) report and efficiently adjudicates credit requests
Training	- Customized content delivered in flexible and meaningful ways to support quick adoption of EIS - Dedicated, experienced training leadership			Trained students in classes

1.1.1 Ordering [L.30.1(1)(a); M.2.2(1 of 3); G.3]

GSA and customer agencies will receive an effective ordering system that accurately and simultaneously supports single orders, large volume orders, new starts, and changes. This level of efficiency will be true throughout the life cycle of the contract but will be particularly evident during the initial years when there is significant transition volume and pressing deadlines to meet. An experienced ordering staff and well-tested ordering systems are necessary to deliver an optimal customer experience for ordering. AT&T has successfully processed large volumes of service

Did You Know?

AT&T has processed more than orders across both of the Network contracts

orders in support of multiple agencies and services using current GSA contracts and will continue to do so in support of EIS. **Table 1.1.1-1** highlights AT&T's approach for order processing on the EIS contract.

Table 1.1.1-1. Ordering Approach and Capability. *GSA and agencies receive flexible and user-friendly ordering support with quality systems and 24x7 access, all built on years of lessons learned supporting Networkx and other GSA and government contracts.*

AT&T Features	GSA and Agency Benefits
▪ The same dedicated and experienced ordering team that has supported the Networkx contracts with the ability to quickly expand knowledge to new products to support EIS ordering.	▪ Reduced transition risk: Lessons learned with Networkx inform more robust ordering systems allowing smooth transition to EIS for Networkx customers
▪ In-place quality controls that will be enhanced to detect EIS ordering issues.	▪ More accurate data feed to GSA enables higher quality ordering process
▪ Disciplined, reliable and repeatable processes for accepting, modifying, and managing TOs, service orders, and GSA contract modifications to EIS.	▪ Enhanced system security: Protects government data ▪ Easy tracking of order status
▪ Agile methodologies used to incorporate upgrades available through our commercial systems provided at no additional charge to the government	▪ Shorter delivery timeframes
▪ Government Center portal through which agencies can enter orders and view order status	▪ Real time order entry and status per planning
▪ Secure File Transfer Protocol (SFTP) API through which GSA can submit orders and receive notification status	▪ Quicker access to new product offerings ▪ Effective, efficient, and low-risk ordering processes
▪ Upload of TO documentation to GSA Systems	▪ Timely updates provided to GSA to enable execution of Agency order needs.
▪ Customizable to meet individual agency TO requirements	▪ Customizable user-defined views of the services ordered
▪ Potential for scripting or other tools to speed like-for-like transitions.	▪ Easier and more accurate quality ordering ▪ Quicker incorporation of EIS technology advances to enhance the customer experience

Orders are accepted only from those authorized on the EIS contract. With decades of experience processing government orders worldwide and across a broad range of services, equipment, and labor, AT&T has the mature processes, flexible systems, and experienced people necessary to meet and comply with the ordering requirements in the EIS RFP.

AT&T will meet and comply with the processes, data, and systems requirements to support and maintain TOs as described in RFP Section J.2.3. This includes but is not limited to the submission of TO summary data and pricing tables and the forwarding of copies of the complete TO. We will not accept a TO or Service Order (SO) or provision services that are not authorized on our contract.

1.1.1.1 Fair Opportunity Process [G.3.1]

GSA or an agency Ordering Contracting Officer (OCO) with a Delegation of Procurement Authority (DPA) will execute fair opportunity procedures in order to issue a competitive TO on the EIS contract. New TOs go through a process as depicted in

Figure 1.1.1-1. An OCO issues an RFP/requests for quotes (RFQ). AT&T will evaluate the requirements and determines the best solution. AT&T will then prepare a proposal, at the sole and exclusive expense of AT&T, that includes all required items and submits to the OCO for consideration. The OCO follows the fair opportunity procedures and exceptions specified in Federal Acquisition Regulation (FAR) 16.505 and enumerated in RFP Section G.3.1 in the RFP.

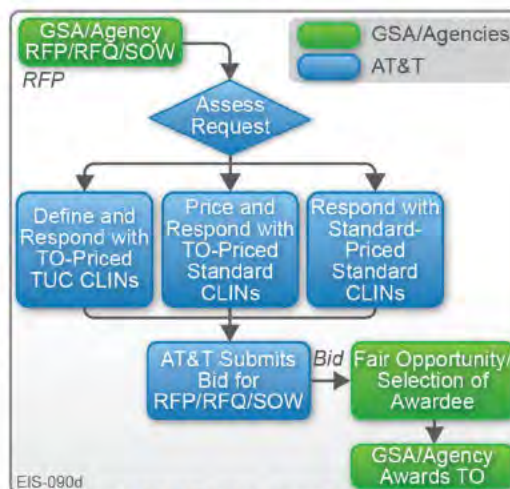


Figure 1.1.1-1. Fair Opportunity Process.

AT&T evaluates and responds to EIS RFP and RFQs in support of the fair opportunity requirements.

1.1.1.1.1 eBuy [G.3.1.1]

AT&T is already registered for access to GSA's eBuy online tool and regularly monitors the site for opportunities. AT&T responds to RFQ/RFPs in the manner prescribed in the request(s).

1.1.1.2 Task Orders [G.3.2]

TOs identify the services required and provide the technical details and scope of work required, including the schedule for all deliverables, the identification of any applicable equipment and labor categories, and service-level performance. TOs may contain a combination of contract line item numbers (CLIN) from the base contract and other agency-specific requirements for services, features, and performance. AT&T will track orders using our BSS throughout the order life cycle. Agencies may require services that, although within the scope of the contract, are not available to order with priced CLINs. In these cases, AT&T will create a Task Order Unique CLIN (TUC) that complies with the TUC pricing submission details described in RFP Section J.4.1. An OCO (or

Table 1.1.1-2. Compliance with TO Process Requirements. *AT&T ordering professionals understand and follow TO processes in support of agency orders.*

Requirement	Achieving Compliance
Task Order Award [G.3.2.1] [G.3.2.4]	The OCO or Contracting Officer's Representative (COR) acting on behalf of the OCO, is the only person authorized to award a TO. The TO may not be modified except by a TO modification issued by the OCO or the OCO designee. A contractor may not accept, and the Government may not award, a task order until the apparent awardee has added all of the CLINs and prices at all locations requested in the agency's solicitation to their contract via fully executed modifications. Any task order issued prior to the execution of all aforementioned modifications will result in the OCO's DPA being revoked
Task Order Modification [G.3.2.2]	AT&T will report all TO modifications to GSA as described in RFP Sections J.2.3 and J.4.
Protests and Complaints [G.3.2.3]	Protests are allowed only on the grounds that the order increases the scope, period of performance, or maximum value of the contract or when a TO is valued in excess of \$10 million. A GSA appointed Ombudsman reviews complaints from contractors and ensures they are afforded a fair opportunity to be considered. The Ombudsman is a senior GSA official who is independent of the GSA Contracting Officer (CO) and OCO.
Fair Opportunity Notice of Protest [G.3.2.3.1]	If protesting a fair opportunity decision, AT&T will provide a full un-redacted copy of that protest to the GSA CO within 3 business days of the protest date. For Freedom of Information Act (FOIA) requests, AT&T will provide a redacted copy to the GSA CO.
Customer of Record [G.3.2.4]	AT&T supports GSA as customer of record on behalf of another agency, GSA acting as the OCO for the agency with the agency remaining the customer of record, and the agency OCO with a DPA acting as customer of record.
Authorization of Orders [G.3.2.5]	. We will not accept a TO, service order, or provision catalog items until the items have been added to the catalog and the discount class has been added to the contract.

designated representative) is the sole and exclusive government official with authority to bind the government. We will not accept or bill the government for TOs or service orders from unauthorized persons. AT&T will verify that the OCO has the required GSA issued DPA [G.2.2.1.1] before accepting TOs. TO modifications may be necessary during the TO period to address requirements or administrative changes.

The OCO for each TO will administer the modifications for that TO. Task order essentials are listed in **Table 1.1.1-2**.

1.1.1.3 Ordering Services [G.3.3]

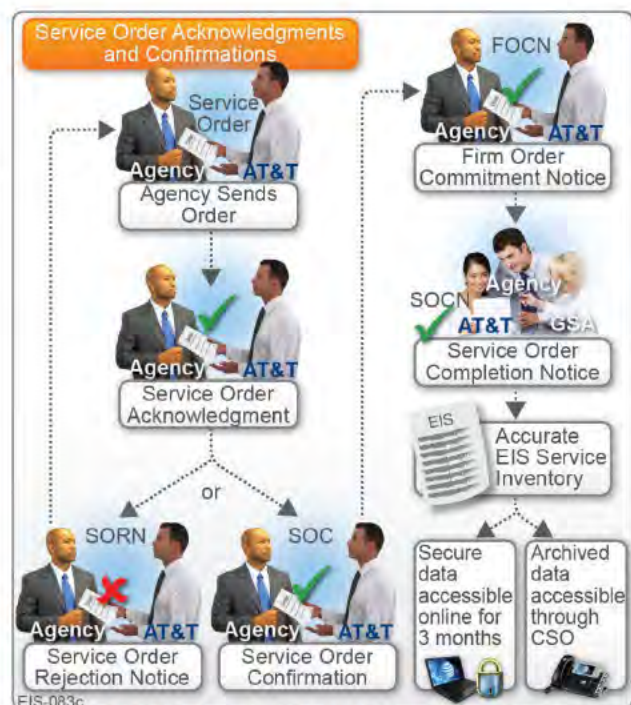


Figure 1.1.1-2. Service Order Flow. *Smooth order flow enables accurate orders, clear status tracking, and completed provisioning of services.*

TOs may generate one or multiple service orders. SOs must be placed against a TO. AT&T will support all service ordering requirements and follow the TO management process as specified in RFP Section G.3.3. **Figure 1.1.1-2** Illustrates the steps in our service order process (for non-rapid, non-self-provisioned services) including the necessary acknowledgements and confirmations needed to maintain the fidelity of the process flow.

In addition, AT&T ordering and notification systems support the required government fields as referenced in RFP Section J.2.4.1 and further addressed in our **Contractor Data Interaction Plan** in **Section 3** of our response. **Table 1.1.1-3** below describes the processes AT&T follows for the required notifications. The transfer mechanism(s) for each includes web services, email (if requested), via the Government Center portal, or other means as agreed to in the TO.

Table 1.1.1-3. Ordering Notices. GSA and agencies receive all required notifications throughout the order life cycle.

Notice Type [J.2.4.1.6]	Process / Frequency to Achieve Compliance	Further Explanation
Service Order Acknowledgment (SOA)	AT&T will submit a SOA within 1 business day of receiving the SO.	Required for Rapid Provisioning services — except if AT&T completes the provisioning process and issues a SOCN within 24 hours of order submission. Also submitted within 1 day of an updated SO.
Service Order Confirmation (SOC)	If AT&T determines that the SO is valid, we will submit a SOC within 5 days of receiving the SO. If the SO is for new service and includes an existing Unique Billing Identifier (UBI), AT&T will create the UBI for the new service with the same service grouping as the provided UBI.	Not required for Rapid Provisioning orders. If changes are required to notifications already submitted, an updated version of the SOC will be issued.
Service Order Rejection Notice (SORN)	If AT&T determines that the SO is invalid, we will submit a SORN within 5 days of receiving the SO. The SORN applies to the entire order. AT&T will not reject individual line items. Exceptions may occur at the written request of the agency while the order is being corrected. If rejected, the government will issue a corrected SO.	If AT&T rejects a Rapid Provisioning order, the SORN will be issued before the lapse of the defined provisioning interval.
Firm Order Commitment Notice (FOCN)	If AT&T must obtain local access services, we will submit a FOCN indicating our Firm Order Commitment (FOC) date from the local provider. If we do not need to obtain local access services, we will submit a FOCN indicating our FOC date no later than the earlier of 5 days after SOC or 10 days before the FOC date. We will submit a FOCN for each provisioning event.	Not required for Rapid Provisioning orders. If changes are required to notifications already submitted, an updated version of the FOCN will be issued.
Service Order Completion Notice (SOCN)	Upon completion of the order, AT&T will submit a SOCN within 3 days of installation and testing unless otherwise specified in the TO. We will submit a SOCN for each provisioning event. We will submit a new SOCN if the government reports a	Required for Rapid Provisioning services.

Notice Type [J.2.4.1.6]	Process / Frequency to Achieve Compliance	Further Explanation
	problem within the acceptance period after it has been fixed and tested.	
Service Order Administrative Change (SOAC)	AT&T will handle administrative data changes to previously provisioned services based on the restrictions and process noted in the RFP.	AT&T issues an Administrative Change Order specifying the inventory items to be changed and issues a SOAC within 7 days. Other order notices are not required.
Service State Change Notice (SSCN)	If a service (defined by a single UBI) changes from one state to another (e.g., an auto sold CLIN has been activated), AT&T will issue a SSCN notice within 24 hours.	AT&T may combine multiple notices as individual line items on a single SSCN — SSCN still submitted within 24 hours or original change.

AT&T will provide agencies and GSA with ordering data on a continuous basis in support of their missions as depicted in **Figure 1.1.1-3**.

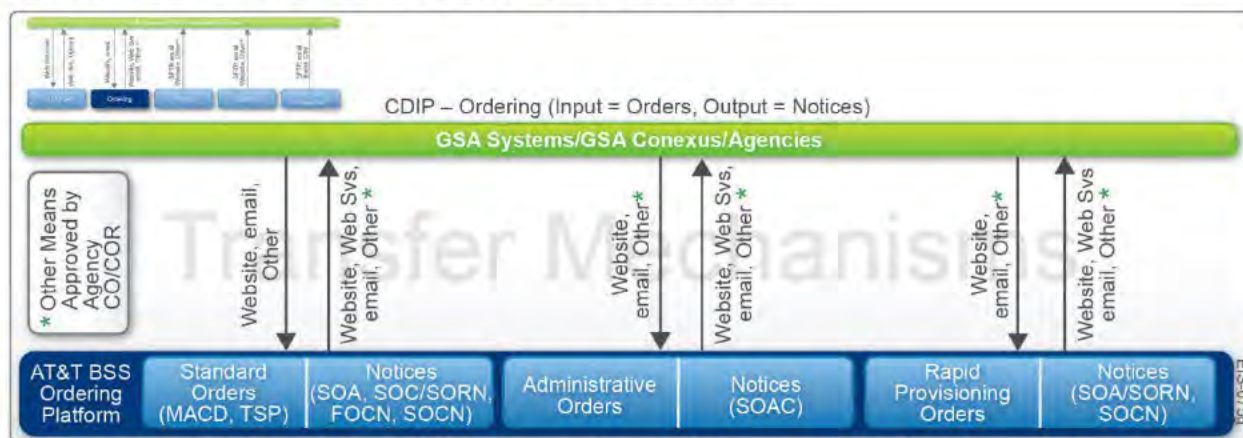


Figure 1.1.1-3. AT&T to GSA/Agencies Ordering Data Interchange. GSA and agencies benefit by accessing our portal 24x7 and user-friendly BSS that provides all required order notices.

In addition to AT&T providing reports and other data, GSA and agencies can access their data through our web-based 24x7 Government Center portal providing access to the BSS. The AT&T BSS is the heart of our ordering solution and is fully compliant with EIS Contractor Data Interchange Requirements. The Government Center portal provides an easy-to-use service order life cycle experience to our customers. GSA and the agencies can place service orders under approved TOs and track all order related reports and notices throughout the order lifecycle. The portal is customizable allowing users to create their own specific view of the data, thus enhancing their ability to support their unique missions. The portal is integrated with all EIS specific tools.

1.1.1.3.1 General Requirements for Ordering Services [G.3.3.1]

AT&T complies with all ordering requirements as described in RFP Section J.2.4. **Table 1.1.1-4** highlights the AT&T general and functional requirements in support of GSA and agency order processing.

Table 1.1.1-4. General and Functional Ordering Requirements. *The Government Center portal and service ordering personnel fulfill all general functional ordering requirements in support of GSA and agency missions.*

General Ordering Requirements	
- Confirm that an OCO has the required DPA before processing TOs - Accept, validate, and complete orders in association with all order requirements - Obtain all needed information to deliver services based on the order and obtaining supplemental information through other sources such as site surveys - Support all order types including adds, moves, changes, cancels, and disconnects - Provide the required order acknowledgements and notifications	
Functional Ordering Requirements (Regarding Placement, Acceptance, and Handling Terms)	
Agency Hierarchy Code (AHC) [G.3.3.1.1]	The OCO provides an authorized and registered AHC for each TO. The AHC is tracked for all services for the life of that service on each order. Because there is no separate charge for services associated with an AHC not registered to the TO, AT&T will validate that each TO has an AHC. AT&T will validate that each order line item has an AHC and reject any order submitted without an AHC for each line item. AT&T will also verify the AHC for each TO CLIN is the AHC provided by the OCO, validate the content of the AHC, if required by the TO, and confirm that changes in the AHC do not interrupt the associated services.
Auto-Sold CLINs [G.3.3.1.2]	Some services include other CLINs that may automatically be included with the original service order. AT&T will include these Auto-Sold CLINs in the proposal or quote just as if they had been explicitly requested in the order. All Auto-Sold CLINs are listed in the notifications and deliverables associated with the order. When new Auto-Sold CLINs are added, AT&T will issue a new SOCN, which will not be applicable to any previously issued TO unless specifically added via TO modification.
Customer Want Date [G.3.3.1.3]	Customer Want Date (CWD) refers to the customer's desired installation date. AT&T will not issue the SOCN nor begin billing before the CWD unless the order specifies that early installation is acceptable. If the time between the order and the CWD is greater than the defined provisioning interval for the service as described in RFP Section G.8.2.2, the servicing provisioning SLA is waived for that service on that order. AT&T will make reasonable efforts to accommodate the CWD.
Service Order Completion Notification (SOCN) [G.3.3.1.4]	No later than 3 days after the completion of each service AT&T will issue a SOCN. After an order has been provisioned and a SOCN submitted and accepted, no revisions to the SOCN are permitted unless one of the following applies: the customer submits an administrative change order, to correct an erroneous submission with the prior approval of the COR, or to add or remove an auto-sold CLIN without an administrative change order.

1.1.1.3.2 Order Types [G.3.3.2]

As depicted in **Table 1.1.1-5** AT&T supports all order types on the EIS Contract.

Table 1.1.1-5. EIS Order Types. *GSA and agencies receive worldwide support as AT&T processes all EIS order types.*

Order Type	AT&T Accepts, Validates, and Completes Requests to Establish New Service
Orders for New Services [G.3.3.2.1]	AT&T will accept, validate, and complete request to establish new service.
Orders to Change Existing Services [G.3.3.2.2]	
Move Orders [G.3.3.2.2.1]	AT&T will accept, validate, and complete move orders, such as network access and/or service related equipment (SRE) moves in the same building (i.e., between floors).
Feature Change Orders [G.3.3.2.2.2]	AT&T will accept feature change orders (that may or may not require a change to the CLIN being billed) to those supplies or services as enumerated in RFP Section B of the RFP. For the mandatory EIS Internet Protocol Voice Service an example of the feature

Order Type	AT&T Accepts, Validates, and Completes Requests to Establish New Service
	change order would be to increase the voice mailbox storage capacity from the basic 60 minutes to 120 minutes.
Disconnect Orders [G.3.3.2.2.3]	AT&T will accept disconnect orders from agencies at any time. Billing for the disconnected services stops on the completion date in the SOCN and within the provisioning intervals for disconnects. Orders to discontinue services are effective 30 or more days from issuance of the order as specified by the government. AT&T will remove equipment related to disconnect orders within 45 days of the termination of services. If equipment sanitization is required, we will remove the equipment within 10 days. If a disconnect order includes the disconnection of services that appear to leave other services effectively unusable (e.g., disconnecting a circuit but not the associated equipment), AT&T will notify the customer of the full list of associated UBIs. AT&T will request clarification of the customer's intent to only disconnect the specified service. If the customer provides instructions indicating that the list, in whole or in part, is intended for disconnect, AT&T will accept this as an order update.
Administrative Change Orders [G.3.3.2.2.4]	Administrative Change Orders (ACO) may only modify inventory data points provided by the government that have no effect on service delivery or pricing. AT&T will accept administrative changes to complete orders, such as updates to AHCs, new points of contact, agency-provided data changes or changes that affect billing, etc. If the ACO specifies inventory items be changed, AT&T will update the inventory database and submit a SOAC within 7 days of the ACO.
Updates to In-Progress Orders [G.3.3.2.3]	
Cancel Orders [G.3.3.2.3.1]	AT&T will accept orders from an agency to cancel a pending order at any step of the order process before the SOCN is issued. Orders may be modified or cancelled by the government during the provisioning process subject to the limitations described in the RFP. When a cancel order renders other services effectively unusable, AT&T will notify the customer of these dependencies and requests clarification of the customer's cancellation intent and responds accordingly. If the customer indicates that the list is intended for cancellation, we will accept this as an order update and request a clarification of the customer's intent to cancel the specified order line items only. AT&T will not charge the ordering agency for network access orders if the cancellation order was placed 30 or more days before the later of the CWD in the initial order or the firm order commitment date.
Location Change Updates [G.3.3.2.3.2]	AT&T will accept location updates that change the service delivery location from that described in the original order (these may or may not influence the location exchange carrier provisioning).
Feature Change Updates [G.3.3.2.3.3]	AT&T will accept updates to features of existing supplies and services as enumerated in RFP Section B.
Customer Want Date Change Updates [G.3.3.2.3.4]	AT&T will accept service/supplemental updates to in-process orders for changes in the CWD from that originally described in the order. If the agency delays the CWD before receiving the FOCN, AT&T will not issue the SOCN and will begin billing before the new CWD, unless the change requested is less than 14 days before the CWD of the initial order.
Administrative Data Change Updates [G.3.3.2.3.5]	AT&T will accept administrative change updates to in-process orders. Administrative data (e.g., service delivery address spelling) is limited to data that does not affect service delivery or pricing.

1.1.1.3.3 Special Order Handling [G.3.3.3]

1.1.1.3.3.1 Telecommunications Service Priority (TSP) Orders [G.3.3.3.1]

AT&T will comply with the requirements for TSP orders. When TSP is specified in the order, AT&T will follow prioritizations applicable to the TSP as required by the order and/or RFP Section G.11. The service is provisioned in accordance with the TSP levels:

- Provisioning priority (5, 4, 3, 2, 1, or E), or
- Restoration priority (5, 4, 3, 2, or 1), or
- Both (provisioning and restoration) as specified in the order from Service Delivery Point-to-Service Delivery Point (SDP).

AT&T will restore service in accordance with the TSP priority levels designated for the transmission service and in accordance with National Communications System Directive (NCSD) 3-1, TSP system for National Security and Emergency Preparedness (NS/EP) and NCS Manual 3-1-1, "Service User Manual for the TSP system".. AT&T will provide expedited service implementation when the ordering agency requires priority provisioning for NS/EP circumstances or other circumstances in which the TSP system is invoked.

AT&T will conduct best efforts to implement the ordered service(s) by the CWD, based on essential priorities as certified by the Department of Homeland Security (DHS) Program. AT&T will notify the government immediately if events arise that have major consequences to the network.

The following Basic Functional Requirements are supported by AT&T for TSP orders [G.11.1]:

- | | | |
|-------------------------------|---------------------|----------------------------|
| ▪ Enhanced Priority Treatment | ▪ Broadband Service | ▪ Nationwide Coverage |
| ▪ Non-traceability | ▪ Affordability | ▪ Voice Band Service |
| ▪ International Connectivity | ▪ Secure Networks | ▪ Scalable Bandwidth |
| ▪ Mobility | ▪ Restorability | ▪ Reliability/Availability |
| ▪ Survivability/Endurability | ▪ Interoperability | |

AT&T will protect classified and sensitive information [G.11.2] that is so identified by the government in accordance with applicable industrial security regulations (National

Industrial Security Program Operating Manual (NISPOM) and National Security Agency (NSA) approved standards as applicable for Safeguarding Classified Information).

AT&T will comply and interoperates with all DHS Office of Emergency Communications (OEC) Priority Telecommunications Services including TSP, Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and when released Next Generation Network Priority Services (NGN-PS) [G.11.3]. OEC's Communications Portfolio Management (CPM) Branch collaborates with the public and private sectors to ensure the NS/EP communications community has access to priority telecommunications and restoration services to communicate under all circumstances.

- AT&T will fully comply with the GETS emergency services directive [G.11.3.1]
- AT&T will fully comply and interoperate with the WPS directive [G.11.3.2]

AT&T will also fully comply with the TSP system's five-level framework (and with any future TSP replacement system) for restoration and provisioning prioritization. If our network experiences significant degradation or failure, AT&T will provide priority restoration of services in accordance with the TSP system and will confirm that the restored circuits maintain the property of the original circuits [G.11.3.3].

1.1.1.3.3.2 Rapid Provisioning Orders [G.3.3.3.2]

As telecommunication services evolve, provisioning become faster, and for many services, agencies "provision" the services themselves. These services lend themselves to rapid provisioning, which streamlines the provisioning process and only requires the SOA and SOCN. Services are subject to rapid provisioning if all of the following conditions apply:

1. AT&T will complete the provisioning process within 48 hours from order placement and will list the service as eligible for rapid provisioning in its proposal
2. The order does not contain a TSP order
3. The order does not contain an ACO

AT&T will add additional services eligible for rapid provisioning at the TO level.

AT&T will not provision and bill for any rapid provisioning services before the CWD unless the order specifies that early installation is acceptable. The proposed provisioning interval will be used to calculate SLA compliance.

Any CWD specified in the order does not apply, and early installation is acceptable.

1.1.1.3.3.3 Task Order Projects [G.3.3.3.3]

Each agency request for service is defined by a TO, which may contain one or more SOs depending on agency requirements. When SOs are grouped the deployment and installation of those services may be sufficiently complex or customized, thus justifying the creation of a TO project. The OCO indicates in the TO requirements if the SOs in the TO are to be managed as a TO project. **Figure 1.1.1-4** delineates the processes we follow once we receive a TO project award.

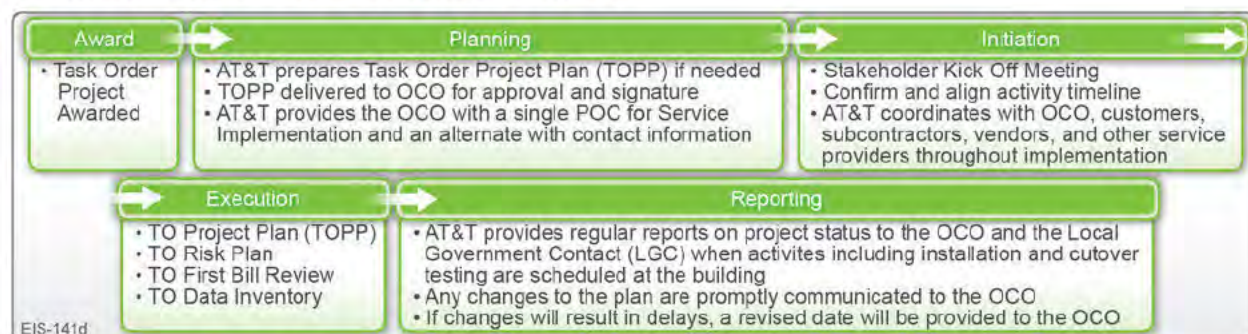


Figure 1.1.1-4. Task Order Project. AT&T TO management processes provide GSA and agencies with responsive and reliable TO project initiation and performance.

Upon award, and at the agency's discretion, AT&T will prepare a Task Order Project Plan (TOPP) that is used to manage the TO project. The TOPP includes the project management elements listed in **Table 1.1.1-6**; however, the OCO may request alternate formats or additional information.

Table 1.1.1-6. TOPP Report Elements. A common TOPP report framework allows for consistency of content and is customizable to agency requirements.

Task Order Project Plan Elements [G.3.3.3.3]	
Common TOPP Elements (Included across all TOs)	
- AT&T primary point of contact for implementing the plan - AT&T escalation contacts (names, phone numbers, emails)	- Name of awarding OCO - TO number
Activities Description of the specific activities required by all parties, including the contractor, the agency, vendors, and the incumbent service provider, to implement the project	Risk Identification of key risk areas for the project, the risk mitigation processes, and contingency plans (when applicable) in the event of the failure of newly installed service
Services Comprehensive inventory of services to be implemented along with SDP, activation date, as-of billing date, testing and acceptance timeframes by contractor and customer, and approach to implementation (hot-cutover, parallel operation, etc.)	Requirements - Specification of government equipment required by location for the effort - Interconnectivity or network gateways required for the effort - Any special technical requirements
Schedule and Billing Installation and service implementation schedule and as-of billing dates	
Site-specific design plan (for location-based service only) to include: Site preparation and implementation requirements for each building. Identify where site surveys will be required; whether surveys will be conducted as physical site visits, telephonically, or other means, and what information will be collected. Indicate what the ordering agency's responsibilities will be for site surveys.	

Task Order Project Plan Elements [G.3.3.3.3]	
▪ Interim and final configuration including hardware (type, manufacturer, model), software, special circuit arrangements, environmental and electrical requirements, equipment room layouts, Main/Intermediate Distribution Frame/riser cable diagrams (if needed), and any special design requirements. ▪ Numbering plan and dialing plan, identifying blocks of telephone numbers, if any, that will have to change. ▪ Interface equipment for Customer Premise Equipment (CPE), including identification and location of special systems integration requirements. ▪ A site-specific cutover test plan that describes AT&T's general approach to cutover testing and pass/fail criteria for each service during service implementation as described here and in RFP Section E.	
Supplemental TOPP Elements (TO-Specific)	
▪ Network map, if applicable, that includes customer addresses, SDP by service type(s), number of lines and trunks. ▪ Proposed approach and physical route to connect each building to the AT&T network, including identification of the number and type of access lines and trunks, if applicable. ▪ Additional information AT&T deems appropriate. Drivers include TO details as well as product/solution details.	

AT&T will deliver the TOPP to the OCO for review and signature approval. The OCO's signature indicates agreement to the implementation schedule and as-of billing date for each item in the TO. For each TO project, AT&T will provide the OCO with a single point of contact (POC) for service implementation, as well as at least one alternate POC. At least one of these individuals will be accessible during the periods when service implementation activities occur. AT&T will coordinate all activities, including with the OCO, agency customers, subcontractors, vendors, and other service providers during the service implementation. AT&T will inform the OCO and the local government contact when activities, including installation and cutover testing, are scheduled. If there is a delay or the installation date changes, AT&T will notify the OCO and provide a revised date.

1.1.1.4 Testing and Acceptance of Services Ordered [G.3.4]

Detailed documentation of well-planned service verification provides a pathway to confirm that services installed perform to the levels required within this contract. AT&T fully complies with the requirements of the verification testing of all associated EIS services based on the GSA methodology described in RFP Section E.2.2. Additional criteria may be included based upon acceptance testing needs defined by an agency within a TO. Greater details on testing and acceptance are found in **Section 2.1** and **Appendices A** and **D** of this volume.

1.1.1.5 Performance Management [G.3.5]

AT&T accepts and complies with the completion timeframes in RFP Section G.8.2.2 associated with the orders of services as defined in RFP Section G.3.3. We address SLA management in detail in **Section 1.1.7**.

1.1.2 Billing [L.30.1(1)(a); M.2.2(1 of 3); G.4]

EIS customers will be provided billing data and online tools to support invoice verification, prompt payment, and invoice analysis necessary for agencies to manage payments and budgets. Billing on EIS includes submission of bill data from AT&T to the government, verification, and validation of the billing data by the government, and proper support of billing disputes and adjustments. Timely and accurate support for all of these functions is paramount for GSA and agencies in support of government budgeting, expense tracking, and validation of proper use of taxpayer funds. AT&T has evolved the EIS billing experience to be flexible, quick, and highly secure for processing and adjudicating agency TO and SO invoices. In addition, as detailed in **Section 3, CDIP** in this proposal response, AT&T is fully compliant with the processes, data, and systems interface requirements described in RFP Section J.2.5. The CDIP is focused on system interface and data structure details.

As shown in **Figure 1.1.2-1**, EIS customers experience the ease and versatility of the AT&T billing application within the Government Center portal, on a secure 24x7 basis, to support implementation of EIS services and to achieve agency business-assurance objectives.



Figure 1.1.2-1. Enhanced Billing Capabilities on EIS. GSA and agencies benefit from increased billing application functionality that provides timely and accurate invoice detail, reporting, and disputes management.

The AT&T billing approach and guiding principles deliver GSA and agencies direct benefits as shown in **Table 1.1.2-1**.

Table 1.1.2-1. Features and Benefits for GSA. Promotes a user-friendly experience by focusing on GSA and agency requirements aiding in mission achievement.

Features	Benefits
Allocation Billing Capabilities	Quickly, simply distribute allocation charges and payments to an agency groups invoiced account that helps subagency cost management
Trending	Faster analysis of evolving trends.
Comprehensive Download Capabilities	Ability to set download preferences as well as download content
Simplified Download Capability	A single download file for all monthly billing details
Ease Changing Hierarchical Structure	Flexible customer-driven hierarchies and access permission levels
Enhanced Payment Reporting	Ability to view invoice balance in HyperText Markup Language (HTML) online at anytime
Paperless	Electronic billing across the platform, supporting designated financials while reducing an agency's carbon footprint
Adjustments and Disputes	Streamlined dispute processing with bulk file upload

The AT&T billing process is fully compliant with EIS requirements and objectives. As seen in **Figure 1.1.2-2**, upon first release of the billing invoice (BI), the Government Center portal enables highly secure, 24x7 access for agency customers.

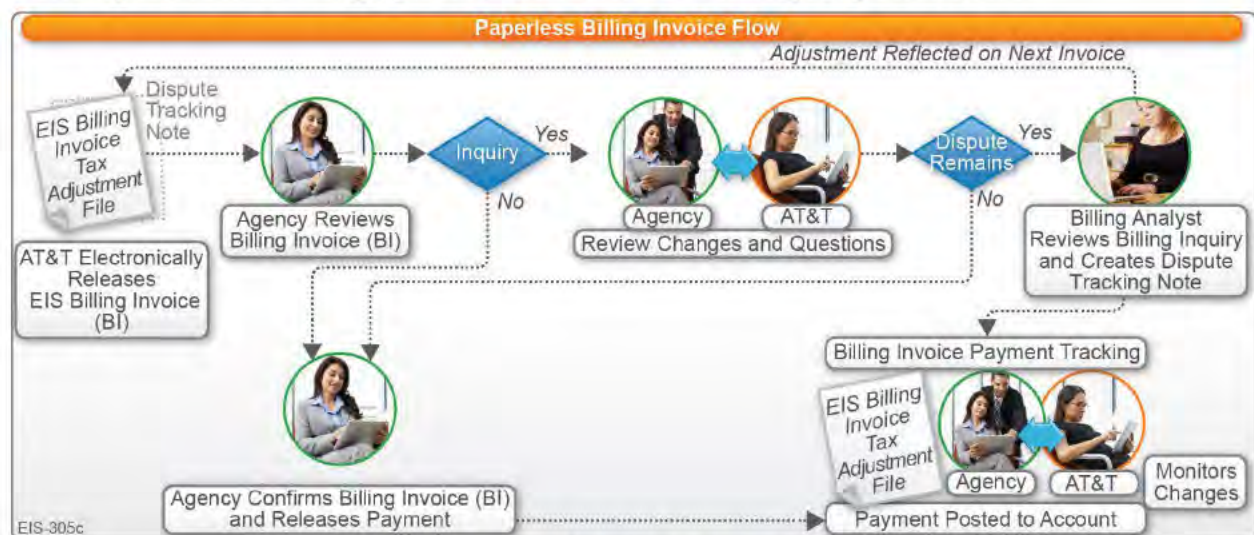


Figure 1.1.2-2. AT&T EIS Billing Process Flow.
Provides timely accurate billing invoices and dispute resolution.

The Government Center billing application provides an easy-to-use interface, resulting in a smooth “no fuss” user experience for customers. Agencies can view billing invoices, dispute resolutions, and payment tracking on approved TOs and track all billing related reports and notices throughout the billing life cycle. The portal is customizable allowing users to create their own specific view of the data, thus enhancing their current ability to support

Did You Know?

AT&T's automated billing systems, supported by skilled billing analysts, have far exceeded Networx billing accuracy SLAs – achieving over [REDACTED] accuracy across both contracts in 2015.

their unique missions. Dispute management tools are also built into the billing application. Below are some examples of functionality that will be available to EIS users. Relevant screen shots are shown in **Figure 1.1.2-3**.

- *Financial Management* accessed via the Government Center Home Page screen allows the user to begin the process of viewing, printing, updating, or creating inquiries based on the user's privileges, which are defined via RBAC. The options available to actual users may be different from what is presented herein, depending upon access defined by the government for RBAC setup.
- *Disputes* accessed from the *Financial Management* menu bar allows tracking of dispute requests by inputting a dispute number.
- Once a customer clicks on the *Disputes* widget he or she also has the capability to find an active dispute by an agency location or by subagencies, and/or by service. This allows a simple means to facilitate dispute confirmation and adjustment invoice validation.



Figure 1.1.2-3. Billing Menu Options. GSA and agencies can click on *Disputes* to view and track inquiries to resolution in real-time.

With decades of experience processing government billing invoices, AT&T has the processes, systems, and experienced people necessary to meet and comply with the billing, inventory, and disputes requirements in the EIS RFP. The subsequent sections demonstrate our full compliance with GSA's billing requirements.

1.1.2.1 Billing Prerequisites [G.4.1]

Table 1.1.2-2 describes the billing prerequisites, processes, functional features, data, and system interfaces that AT&T uses for the required billing invoice submissions, verification and validation, and disputes and adjustments reports and notifications. AT&T invoices are based on the inventory generated through issuance of a successful SOCN and billing adjustments received from the billing disputes and adjustment tool. The invoice represents charges billed within 90 days of issuing the SOCN with no duplication.

Table 1.1.2-2. Billing Processes, Data and System Interfaces. GSA and agencies receive all required notifications throughout the billing life cycle. [G.4.1, J.2.5]

EIS Billing Requirement	Functions/Frequency	Compliance Notes
Billing Cycle [G.4.1.1]	- AT&T will comply with the government's billing period, which runs from the first through the last day of the calendar month. - Billing will be in arrears at the end of every month after providing services. - All billing will be rendered based on calendar month cycles.	- In compliance with RFP Section J.2.5.1.1 requirements - In compliance with RFP Section J.2.5.1.5 requirements
Billing Start Date and End Date [G.4.1.2]	- AT&T will submit a SOCN to the government before billing for associated services. - AT&T will initiate billing with the completion date noted on the SOCN. The completion date is the billing start date for new services and billing end date for disconnected services. - Billing will not begin for services if the government rejects the services within 3 days of the SOCN. - If the SOCN is rejected, AT&T will issue a new SOCN with an updated completion date after correcting the reasons for rejection.	- AT&T will comply with billing start date requirements specified in the TO, provided the adjustment does not violate the 90-day billing requirements described in RFP Section G.4.1.3. - A TO may also specify alternate billing start date requirements provided the adjustment does not violate the 90-day billing requirement described in Section G.4.1.3. In such cases, AT&T will comply with the billing start date requirements specified in the TO. - Unless otherwise noted in the TO, non-recurring charges (NRC) are the same as those in effect when the order was placed. - For Monthly Recurring Charges (MRCs) the price billed corresponds to the price in effect for that month.
90-Day Billing Requirement [G.4.1.3]	- AT&T will invoice services charges up to 90-days after issuance of the SOCN across all services. - AT&T accepts payments for invoices issued after the 90-day window when the GSA CO or agency OCO waive the billing requirement on a case-by-case basis.	- AT&T will invoice service charges within 90 days after issuance of the SOCN across all services, SREs, and inclusive of usage and non-usage services. - This 90-day requirement applies to both initial invoicing and all billing adjustments.
Unique Billing Identifier [G.4.1.4]	- During the Service Ordering process, AT&T will create the UBI as described in RFP Section J.2.10.1.1.2. - We will assign a UBI for each billed record and provide to all components of the billed services	AT&T will verify that the UBI reporting on the billing deliverables matches the UBI included in the SOCN.

EIS Billing Requirement	Functions/Frequency	Compliance Notes
Agency Hierarchy Code [G.4.1.5]	AT&T will validate the inclusion of an AHC on each line item to be processed for billing and will support AHC changes to provisioned services without interruption of service.	AT&T has provisions in place to validate the AHC upon request of the TO. The billing and charges will also be subject to pre-bill validation as part of the AT&T bill cycle close procedures.
Agency Service Request Number [G.4.1.6]	If the government provides an Agency Service Request Number (ASRN) AT&T will include the ASRN data in billing records throughout the service lifecycle.	- ASRN(s) are supported in the operations and billing. The ASRN will contain customer specified data: for example, Customer Service Authorization (CSA) and Telecommunications Service Request (TSR) numbers. - The invoice processing distribution platform can be customized to meet agency-specific financial system interfaces, if required within TO(s).
Electronic Billing [G.4.1.7]	- AT&T will provide electronic invoicing for all TOs. - In addition, AT&T supports input summary data into the government systems noted in RFP Section G.4.1.7.	- The invoice processing distribution platform can be customizable to meet the customer financial system interfaces. - Support includes systems for WebVendor, Vendor and Customer Self Service (VCSS) system, and Invoice Processing Platform (IPP)

1.1.2.2 Direct Billing [G.4.2]

Agencies will receive an invoice directly from AT&T for all charges incurred by the respective agencies and its subagencies. AT&T will be paid directly by the agency.

AT&T will collect the AGF from the direct-billed agencies and remit the total AGF amount collected for the month to GSA via electronic funds transfer (EFT).

1.1.2.3 Billing Functional Requirements [G.4.3]

In addition to complying with the functional requirements described in RFP Section G.4.3, AT&T complies with the processes, deliverables, and data exchange requirements defined in RFP Section J.2.5. The AT&T CDIP, included herein as **Section 3**, provides details regarding AT&T's compliance.

AT&T responds within seven days to a billing inquiry. The billing inquiry can be submitted to AT&T via phone or via the disputes application within the Government Center portal. The disputes application allows the agency to view, update, create an inquiry, and display the total inquiries outstanding for the user. Resolution of billing disputes is supported by the AT&T billing organization, which is aligned to support GSA and agencies.

Did You Know?

AT&T's automated billing system has the capability to provide secure, electronic bonding with customer portal(s) providing a paperless, dependable, efficient, and repeatable user experience.

1.1.2.3.1 Adjustments [G.4.3.1]

If AT&T needs to adjust a bill, the approved adjustment is processed and applied to the next available bill. If an adjustment is requested due to a dispute, we follow the process in **Section 1.1.2.4** and comply with CDIP requirements from RFP Section J.2.5 as discussed in **Section 3**.

1.1.2.3.2 Monthly Billing Informational Memorandum [G.4.3.2]

GSA and agencies are provided AT&T personalized messages to clarify any line items on the billing invoice. Messages are sent monthly and delivered no later than (NLT) the 15th business day of each month. The Monthly Billing Informational Memorandum explains changes in billing, data format changes, new services added to the billing, issues pertaining to balancing charges, or other explanations as required, and is provided monthly to coincide with the monthly delivery of billing files.

Did You Know?

AT&Ts enhanced automated billing system will deliver clear, consolidated, accurate invoices the first time, every time, on time.

1.1.2.4 Disputes [G.4.4]

Should the GSA CO, an OCO, or another authorized user need to issue a dispute against a BI, an Inventory Reconciliation (IR), or an SLA Credit Report (SLACR) response previously provided, AT&T will accept and process the dispute(s). AT&T will comply with the processes, deliverables, and data exchange requirements in RFP Section J.2.6 (and detailed in **Section 3.6**). Via AT&T's billing team, we will resolve all disputes within 180 days of the dispute notice. AT&T understands that the government reserves the right not to make payment for disputes that have not been resolved within 180 days. Any resulting adjustments will appear on a subsequent invoice.

1.1.2.4.1 Billing Disputes Resolution [G.4.4.1]

Within seven days of receipt of a bill, the government may reject a bill in whole or part. This begins the billing dispute process. AT&T will work directly with the appropriate agency to resolve the dispute within 180 days of the dispute notice. Partial resolutions are allowed and may be accepted or rejected by the agency. The OCO responds to proposed resolutions within 14 days. If a partial resolution is accepted that adjustment is made and the unresolved portion of the dispute remains open. Disputes may be escalated to the OCO as appropriate at any time however, unless there is an agreed

upon extension, disputes that are not resolved within 180 days will be escalated. Escalated disputes to an OCO are resolved in accordance with FAR 52.233-1 (Disputes). The dispute process ends when AT&T submits a corrected bill (with appropriate debit or credit) and the associated billing dispute identifier or the agency withdraws the dispute. We will document all disputes according to the RFP Section J.2.6, in the monthly Dispute Report (DR). GSA and agencies will receive notification throughout the dispute life cycle as referenced in **Figure 1.1.2-2, AT&T EIS Billing Process Flow**.

1.1.2.5 Payment of a Bill by the Government [G.4.5]

The government will pay AT&T only for items and services delivered within the procedures defined for EIS. AT&T will deliver timely, accurate monthly invoices for government review and payment. Upon expiration of the contract or TO, AT&T will submit a final billing invoice for direct-billed services within 90 days, unless the OCO has granted an extension in writing. Invoices are not final until all payments have been processed. The final bill is posted once all account activity has been processed and account brought to a zero balance.

1.1.2.6 Associated Government Fee [G.4.6]

AT&T will collect the AGF for the customer agencies monthly throughout the life of the contract and will remit the collected fees monthly via EFT to GSA. The AGF percentage rate and AGF amount will be reported on the monthly billing invoice data set deliverable.

1.1.2.7 General Billing Requirements

AT&T will comply with all billing requirements as described in RFP Sections G.4.7-G.4.12.2. **Table 1.1.2-3** highlights AT&T processes in support of GSA and agencies billing requirements.

Table 1.1.2-3. Additional Billing Requirements. CSO Service Ordering personnel ensure all general functional ordering requirements are fulfilled in support of GSA and agency missions.

Additional Billing Requirements	
Billing Requirements	AT&T Response
Electronic Funds Transfer [G.4.7] Government Purchase Card Payments [G.4.8]	- AT&T strongly encourages use of EFT and will provide agencies with all customer setup and banking instructions. - At the TO level, we will provide the information in coordination with the designated agency bank to process government card purchases.
Rounding of Charges for Billing and AGF [G.4.9] Proration of Monthly Charges [G.4.10]	AT&T will comply with billing requirements including but not limited to rounding of

Additional Billing Requirements	
Billing Requirements	AT&T Response
Taxes, Fees and Surcharges [G.4.11] Separate Billing of Taxes, Fees and Surcharges [G.4.11.1] Aggregated Taxes [G.4.11.2]	charges, proration, aggregated taxes, separate billing of fees and surcharges.
Billing Performance Objectives [G.4.12] Billing Data Accuracy Key Performance Indicator [G.4.12.1] Billing Charges Accuracy Key Performance Indicator [G.4.12.2]	- AT&T will submit accurate billing that meets all performance objectives required in RFP G.4.12, Billing Performance Objectives. - AT&T will meet or exceed the 95% Acceptable Quality Level (AQL) for the Billing Data Accuracy Key Performance Indicator (KPI) as calculated per RFP Section G.4.12.1 and the Billing Charge Accuracy KPI as calculated per RFP Section G.4.12.2.

In summary, GSA and agencies will receive AT&T billing data that complies with all functional requirements in RFP Section G.4 in support of their missions. AT&T will process fully compliant billing invoices for services, equipment, and labor worldwide.

Figure 1.1.2-4 depicts an overview of the AT&T integrated Billing process flow.

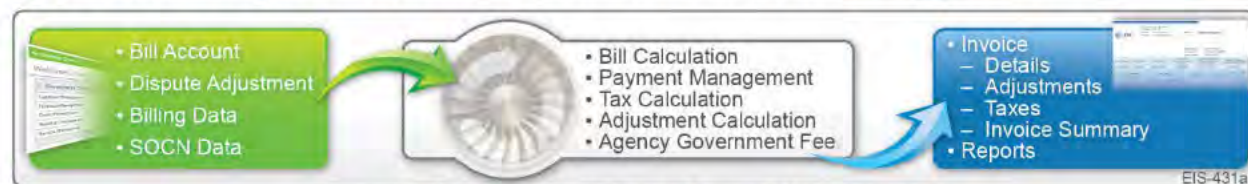


Figure 1.1.2-4. Integrated Billing View. AT&T only provides billing data to authorized users of the EIS contract.

1.1.3 Business Support Systems [L.30.1(1)(a); M.2.2(1of 3); G.5]

Web-based, real-time BSS and experienced support personnel will provide GSA and agency customers a user-friendly experience. AT&T is investing in the Business Center portal to enhance various features for EIS compliance to provide an effortless experience with AT&T's BSS functions and capabilities.

The insights that data can provide are only as good as the flexibility and compliance of the tools through which that data is accessed. GSA and agencies fulfill critical missions by using our integrated BSS. In support of EIS, AT&T will combine our knowledge of Networkx customer needs with the requirements specific to the EIS contract and provide our customers with enhanced, web-based access to the BSS. The AT&T BSS solution provides a single, web-based, highly secure portal through which agency customers can access the BSS applications.

Did You Know?

AT&T's web-based support system (BusinessDirect®) for our commercial and government customers process more than 63 million transactions annually.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Our flexibility and long-term commitment fosters support for the government's evolving requirements related to functionality, IT Governance, National Institute of Standards and Technology (NIST) standards, and Federal Information Security Management Act (FISMA)-based security requirements. AT&T's Business Center portal and the BSS behind the portal are designed to provide EIS users with a positive experience for ordering, access to the pricing catalog, trouble ticketing, inventory management, billing and payment management service management, customer support, dispute resolution, and overall program management activities. Our BSS target platform architecture, shown in **Figure 1.1.3-1**, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

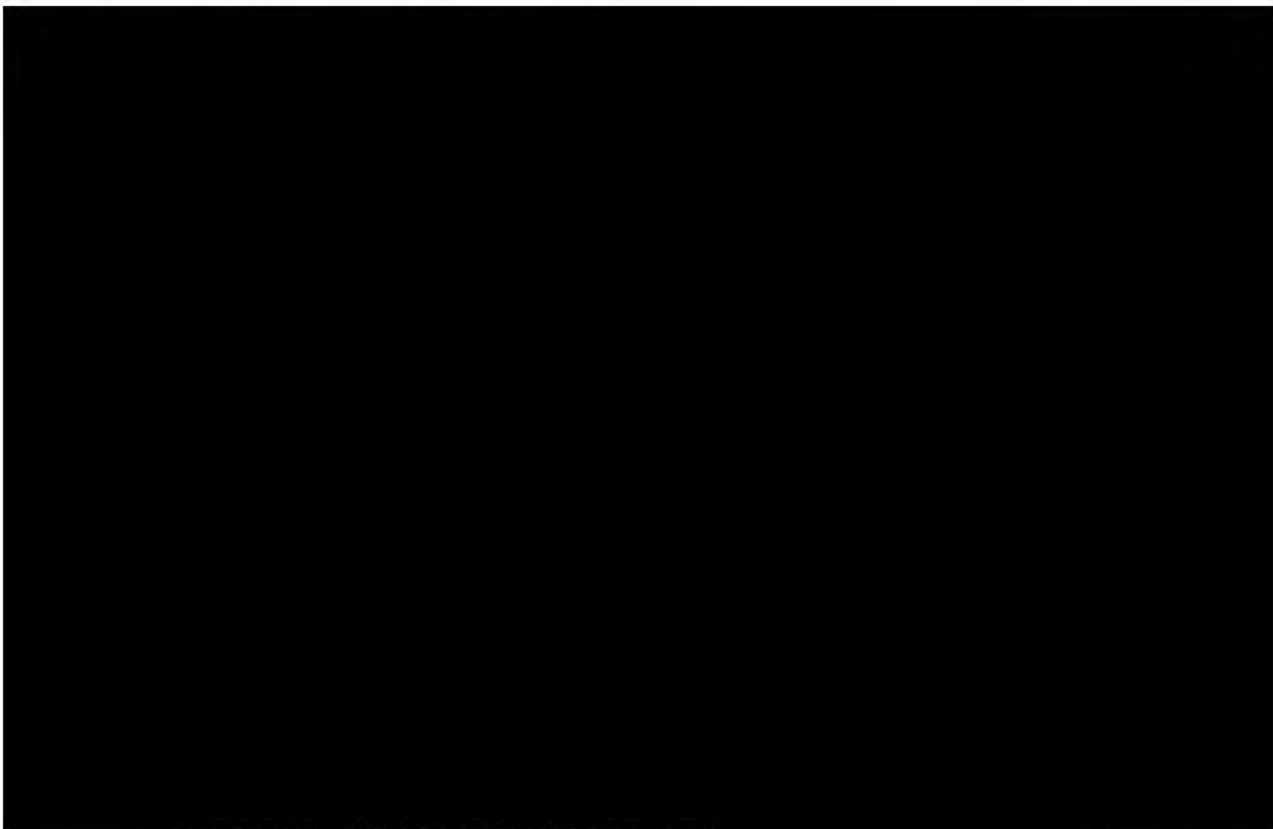


Figure 1.1.3-1. AT&T Future Target Architecture.

The welcome page of the Business Center portal, as seen in **Figure 1.1.3-2**, represents the AT&T investment in the next generation of the AT&T BusinessDirect® portal that currently processes more than [REDACTED] million transactions annually for our commercial and government customers.

Customized applications for EIS support GSA and agency requirements while offering users an effortless experience with access to superior commercial capabilities with enhancements to support the unique characteristics of government requirements. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

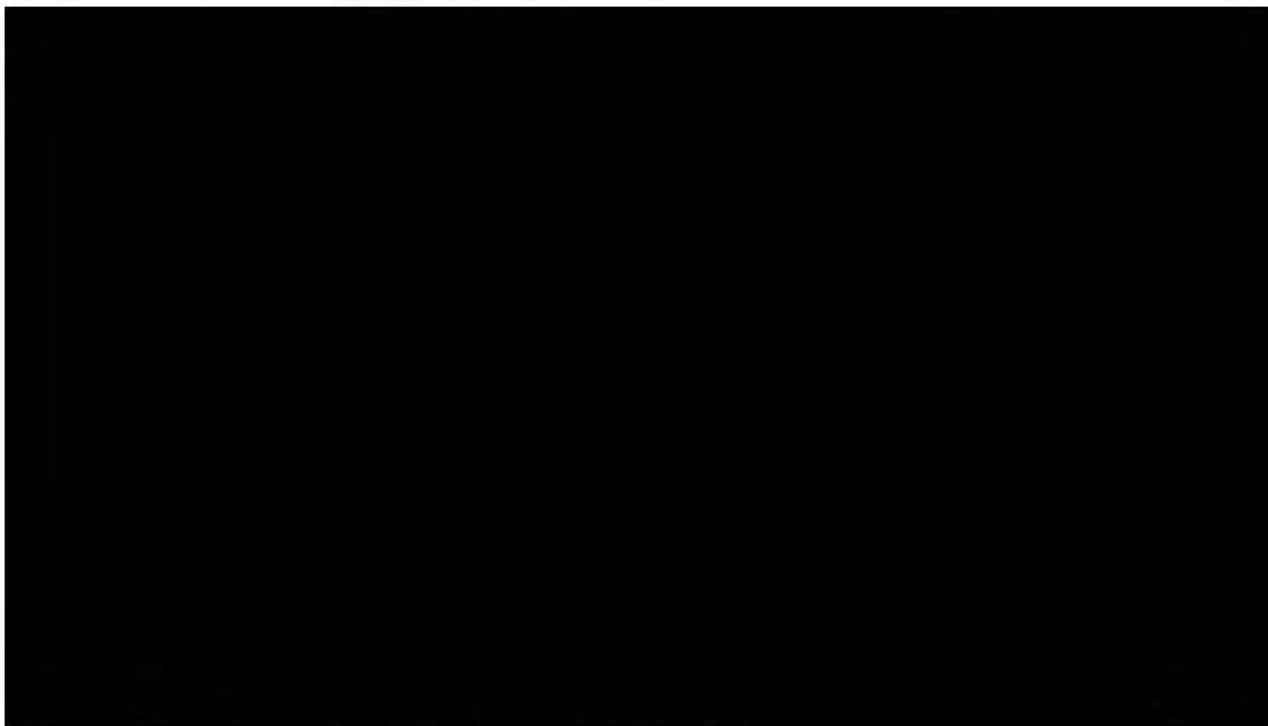


Figure 1.1.3-2. AT&T Business Center Portal Example.

AT&T's combined BSS and web portal design offer many features that benefit GSA and the agencies, several of which are described in **Table 1.1.3-1**. AT&T is confident these enhanced features will bridge current and future technologies, user demands, and meet security needs for the duration of the EIS program.

Table 1.1.3-1. AT&T Web-based Systems BSS Features and Benefits.

AT&T Features	GSA and Agency Benefits

1.1.3.1 Overview [G.5.1]

AT&T's BSS currently support enterprise and government customers across a broad spectrum of industries. As requested in RFP Section G.5.1, AT&T will use its commercial systems to meet the EIS BSS requirements for service delivery and service assurance. [REDACTED]

Using the concepts currently in place with AT&T's commercial systems, the new Government Platform will provide user-friendly, compliant, and efficient support systems, including service ordering, operational support, billing, inventory, SLA management, trouble handling, training, and customer service.

AT&T will use our Networx BSS experience, customer feedback, government, and industry best practices, as well as, information gleaned from our involvement in the American Council for Technology/Industry Advisory Council (ACT/IAC) to offer an improved customer experience with the EIS BSS Business Center portal. This collaboration supports our continuous improvement that results in improved quality, access, and overall utility for EIS customers.

1.1.3.2 Technical Requirements [G.5.3]

As we discuss in the following sections, AT&T's BSS is designed to meet or exceed all the technical requirements stipulated in RFP Section G.5.3. In addition to providing a user-friendly web interface for BSS functions, AT&T will provide web services for direct data exchange and SFTP-based data transmission for large deliverables.

1.1.3.2.1 Web Interface [G.5.3.1]

In addition to the minimum functions specified in RFP Section G.5.3.1.1, as discussed below, AT&T's Government Center will provide access to several BSS functions

[REDACTED]

[REDACTED] Training associated with use of our highly secure, user-friendly web interface/portal is discussed in **Section 1.1.8**.

1.1.3.2.1.1 Web Interface Functions [G.5.3.1.1]

The Government Center portal, with the inclusion of service management, exceeds the minimal functional requirements noted in RFP Section G.5.3.1.1 and will provide access to the BSS functions as shown in **Figure 1.1.3-3**. Each of our functional modules directly correlate to the requirements defined in RFP Section G.5.4.



Figure 1.1.3-3. AT&T's BSS Web Interface Functions.

1.1.3.2.1.2 Technology Standards [G.5.3.1.2]

AT&T's web-based BSS will adhere to common industry standards. In the interest of supporting a wide array of web browsers, AT&T's BSS will not require special software or plug-ins beyond standard web browsers with default built-in functionality. The BSS will support the following web browsers in their current and most recent versions (N-1) as well as any successor products:

- Microsoft Internet Explorer/Microsoft Edge (desktop and mobile)
- Mozilla Firefox (desktop and mobile)
- Apple Safari (desktop and mobile).
- Google Chrome (desktop and mobile)

1.1.3.2.1.3 Accessibility [G.5.3.1.3]

The Corporate Accessibility Technology Office (CATO) leads AT&T's efforts to address the needs of individuals with disabilities in the design and development of our enterprise products and services. CATO collaborates with each business unit within AT&T to advance AT&T's efforts to comply with the accessibility requirements for all customer facing products, services, networks, and websites.

AT&T uses [REDACTED] [REDACTED] to adhere to compliance with Section 508 of the Americans with Disabilities Act and Web Content Accessibility Guidelines (WCAG). To make our solutions accessible to the widest possible population of disabled users, AT&T follows a comprehensive accessibility testing approach including automated testing with state-of-the-art toolsets,

[REDACTED] All EIS BSS applications will be 508 compliant per RFP Section G.5.3.1.3.

To demonstrate compliance we will provide a comprehensive list of all offered Electronic Information Technology (EIT) products (supplies and services) that fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. AT&T will post this list using the applicable Voluntary Product Accessibility Template (VPAT) to our website (www.att.com/gov/eis) within 30 days of Notice to Proceed (NTP). If AT&T must offer a product that is not fully compliant, that information will be indicated in that particular VPAT to assist the procurement official in making a determination based on market research of the most compliant product that meets the agency's needs. That VPAT will indicate the degree of compliance with applicable product technical and functional standards and document any exceptions.

1.1.3.2.2 Direct Data Exchange [G.5.3.2]

In addition to web-based access to BSS systems, AT&T BSS will support highly secure, automated mechanisms for direct transfer of detailed transaction data that includes all elements detailed in RFP Section G.5.4 to GSA Conexus using Web Services and SFTP as stipulated in RFP Section G.5.3.2.1.

The CDIP in **Section 3** provides a more detailed account of the direct data exchange solution for EIS. **Figure 1.1.3-4**



Figure 1.1.3-4. Contract Data Interaction Plan (CDIP) High-Level Process Flow.

1.1.3.2.2.1 Direct Data Exchange Methods [G.5.3.2.1]

AT&T's BSS is designed to support the direct data exchange methods for system-to-system data exchange of transactions, attachments, and large files with Conexus as Stipulated in RFP Section G.5.3.2.1. That includes both web services and SFTP Services as follows:

- **Web Services** — Bidirectional transactions over Hypertext Transfer Protocol Secure (HTTPS) via APIs that support XML over HTTPS using Simple Object Access Protocol (SOAP) as the web services exchange protocol. The web services will use X.509-based digital certificates to support mutual authentication and encryption and observe the NIST Special Publication (SP) 800-95 (Guide to Secure Web Services) as well as other references identified in NIST SP 800-53 R4 and GSA Web Application Security Guide 07-35.

- **Secure File Transport Protocol (SFTP) Services** — Bidirectional transactions for file-based data exchange between government provided File Transfer Protocol (FTP) services and AT&T BSS using Pipe-Separated Value (PSV) exchanged via a server operated by or on behalf of GSA.

AT&T's BSS will submit any Binary Large Object (BLOB) attachments required in the definitions of the various data sets as discussed in RFP Section J.2.10.2. These BLOBs will be separately transmitted via SFTP as described above and in CDIP (**Section 3**) and will comply with the template specified in RFP Section J.2.9.2.2.

1.1.3.2.2.2 Direct Data Exchange Formats [G.5.3.2.2]

The AT&T BSS will accept data transfers from the government and submit data to the government using XML and SFTP formats as specified in RFP Section J.2.9.

1.1.3.2.2.3 Direct Data Exchange Governance [G.5.3.2.3]

AT&T understands that GSA will maintain and manage all approved data exchange format specifications, data schemas, and method descriptions and that the agency customer may include additional customer data exchange requirements in a TO. After the BSS is operational any changes or updates to the data exchange formats or methods and timeframes for implementation will be coordinated and negotiated with the government and subject to the BSS change-control process specified in RFP Section G.5.5.1.

1.1.3.2.3 Role Based Access Control (RBAC) [G.5.3.3]

As part of the initial setup and ongoing maintenance of TO data in GSA Conexus and AT&T BSS, AT&T will collect from the government customer the list of users and user permissions to setup access control to BSS functions and government data.

AT&T will allow only authorized users with appropriate permissions to access BSS functions, including the ability to place orders and access order status, billing, inventory, and performance information. AT&T will capture and store the authorized permission settings to prevent unauthorized user access restricted data. In collaboration with the government, AT&T will add new users within seven days of customer request and will remove users who are no longer authorized in one business day of notification.

1.1.3.2.4 Data Detail Level [G.5.3.4]

The AT&T BSS will fully comply with the data detail, format and transfer mechanisms specified in RFP Sections G.5.3.4 and J.2. AT&T will provide all data elements relating to the services listed in RFP Section G.5.4, BSS Component Service Requirements as addressed in RFP Section J.2. As required in RFP Section J.2, all BSS deliverables and reports will be submitted in the following formats:

- **Human-Readable** — Via AT&T Business Center portal, email for unstructured data with Microsoft Office or Portable Document Format (PDF) attachments
- **Machine-Readable** — As part of the direct data exchange via web services or SFTP.

1.1.3.3 BSS Component Service Requirements [G.5.4]

The AT&T's Government Center portal will provide access to not only the required web interface functions [G.5.3.1.1], [REDACTED]

[REDACTED] Figure 1.1.3-3.

1.1.3.3.1 BSS Component Service Requirements Table [G.5.4.1]

[REDACTED] Figure 1.1.3-3.

1.1.3.4 BSS Development [G.5.5]

1.1.3.4.1 BSS Development and Implementation Plan [G.5.5]

This BSS Development and Implementation Plan incorporates the procedures as detailed in our approved BSS Verification Test Plan, our BSS Risk Management Framework Plan and BSS System Security Plan (SSP). Incorporating these plans by reference creates a comprehensive plan for BSS development, testing, and implementation.

Figure 1.1.3-1 indicates the [REDACTED] architecture for our BSS. AT&T is investing in the development of our EIS BSS and understands the government will not pay for the development or maintenance of the BSS and that we are responsible for all development, testing, and maintenance including but not limited to, security validation, functional testing, upgrades, and configuration control.

Building on the lessons learned from operating our Network BSS for the last eight years

[REDACTED] Our timeline, as indicated in **Appendix A, Section A-3**, is to achieve authority to operate approximately [REDACTED] days

after notice to proceed is received. Some salient points regarding the development approach and timeline include:

- Per GSA's guidance in RFP Section G.5.1, AT&T will use its commercial systems to meet GSA's new EIS BSS requirements.
- AT&T will provide highly secure systems such as Customer Management, Financial Management,
- AT&T's Technology Development organization uses a process for BSS development to speed up the turnaround time within the Software Development Life Cycle methodologies employed by AT&T, such as

Figure 1.1.3-5

Figure 1.1.3-5. AT&T's Continuous Delivery Process.

Using software development methodologies to build and or enhance applications in an iterative and incremental manner will enable us to build and enhance our BSS platform that is fully compliant with customer needs and delivers within budget and on schedule. The BSS Development, Test and Implementation timeline for the AT&T BSS project is shown in **Figure 1.1.3-6**.

1.1.3.4.2 BSS Change Control [G.5.5.1]

AT&T uses industry-standard development and change-control tools and processes, including

AT&T will comply with the BSS change-control requirements, as defined in RFP Section G.5.5.1, specifically for any web interface changes that affect Section 508 compliance or require additional user training, changes to direct data exchange, ability of BSS to meet any specified requirements, and system security. AT&T will provide a BSS change-control notification to the government at least 30 business days before all BSS changes regardless of their impact. In the event of an emergency change, AT&T will provide this notice as soon as the need for it is detected. For updates subject to change control, AT&T will obtain government approval, use industry standard procedures, train government personnel as required, retest functionality and update change information within 7 days.

1.1.3.5 BSS Security Requirements [L.30.2.7; M.2.2(7of 8); G.5.6]

In order to meet critical security requirements our security organizations are dedicated to the physical and logical security of the global network, its service offerings, and

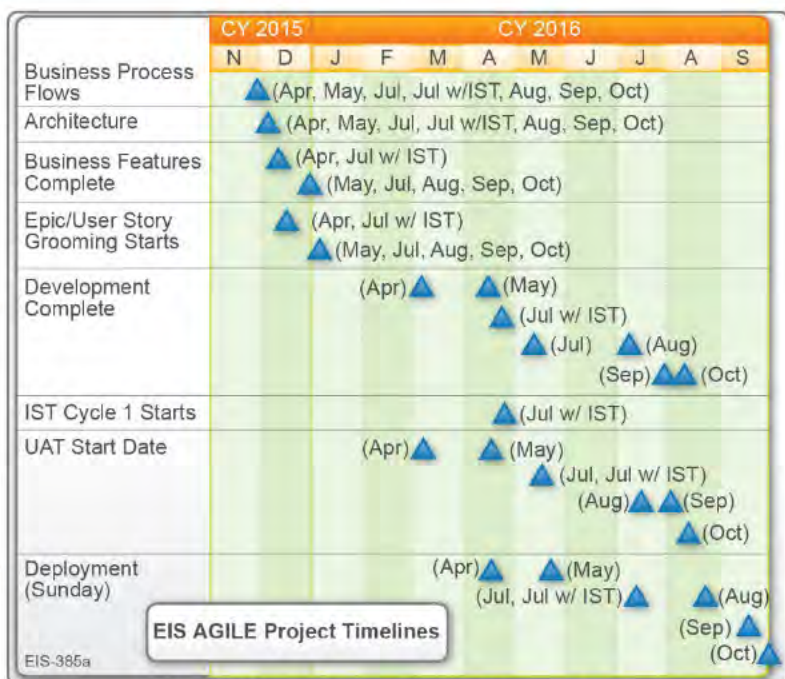


Figure 1.1.3-6. AT&T BSS Development, Test and Implementation timeline. Based on an Agile methodology, AT&T is confident of meeting critical milestones and is currently on schedule to fully develop and implement our BSS.

Business Support Systems. AT&T's BSS will comply with the EIS security requirements specified in RFP Section G.5.6.

AT&T software and system architects approach security concerns strategically, as they view security as an integral part of the solution. This

Did You Know?

AT&T's Network CSO provides technical support to [REDACTED] subagencies representing more than [REDACTED] service orders.

"security first" mindset drives our BSS functional design and development. AT&T's Security Policy and Requirements (ASPR), an ISO Certified Security Policy, provides a framework that is adopted from the beginning of the development process. In addition to ASPR, AT&T will also implement the BSS to meet all applicable FISMA directed NIST and Federal Information Processing Standards (FIPS) guidelines and follow GSA IT Security directives through the entire system life cycle. AT&T will support the government's efforts through the Security Assessment and Authorization (A&A) process to verify we are meeting these standards to receive an Authority to Operate from GSA. AT&T understands and will comply with the applicable federal and agency specific IT security directives, standards, policies, and reporting requirements. This includes, but is not limited to, FISMA guidance and directives to include FIPS, NIST Special Publication (SP) 800 series guidelines, GSA IT security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of government IT systems and infrastructure. We will document all AT&T-implemented settings in the Contractor Implemented Settings workbook, Column E, that are different from GSA-defined settings and where deviations are allowed. Compliance includes all requirements referred to in RFP Sections G.5.6.1, G.5.6.2, and G.5.6.4. AT&T will provide any ISAs for the information system with the initial security A&A package to include annual updates. As part of our compliance process, we are submitting **Appendix G** to our proposal. Our BSS SSP, which will be delivered within 30 days of NTP, will contain the RFP Section G.5.6 compliance details and will comply with all security Assessment and Authorization (A&A) requirements.

1.1.3.6 Data Retention [G.5.7]

AT&T will comply with FAR Subpart 4.7 (48 CFR 4.7) and maintain an archive of all records for three years after final payment under the contract. To meet this objective,

AT&T's corporate Records and Information Management (RIM) policy will include a new retention series code for all applicable EIS records.

1.1.4 Customer Support Office and Technical Support [L.30.1(1)(a); M.2.2(1 of 3); G.6]

GSA and customer agencies will receive superior customer service built upon lessons learned serving [REDACTED] agencies and [REDACTED] subagencies on the Networx contracts, as well as supporting other GSA customers and LSA contracts. Our systems and processes are evolving to best support EIS requirements now and throughout the life of the contract.

1.1.4.1 Customer Support Office [G.6.1]

The requirements defined in RFP Section G.6 are included in our discussion within the CSO which also includes service assurance elements, Supply Chain Risk Management (SCRM), trouble ticket management, and service assurance functions.

The AT&T CSO is our dedicated program management organization responsible for all aspects of AT&T's EIS program and is the primary interface between AT&T and the government using the EIS contract. [REDACTED], AT&T EIS Program Manager, provides leadership to our CSO and a continuity of program knowledge that will be helpful in transitioning customers from Networx to EIS.

As depicted in **Figure 1.1.4-1**, AT&T's EIS CSO is designed to provide the GSA and agencies fully compliant and efficient service delivery and support to both GSA and AT&T for successful EIS contract performance. **Figure 1.1.4-2** depicts communication channels between the CSO and GSA, AT&T service delivery organizations, and agencies. The entire structure as illustrated in **Figures 1.1.4-1** and **1.1.4-2** is designed to support the delivery of AT&T high-quality secured services to agencies around the world. The left side of **Figure 1.1.4-2** depicts CSO interfaces with GSA and the right side depicts the AT&T functional alignment to support agency specific requirements.

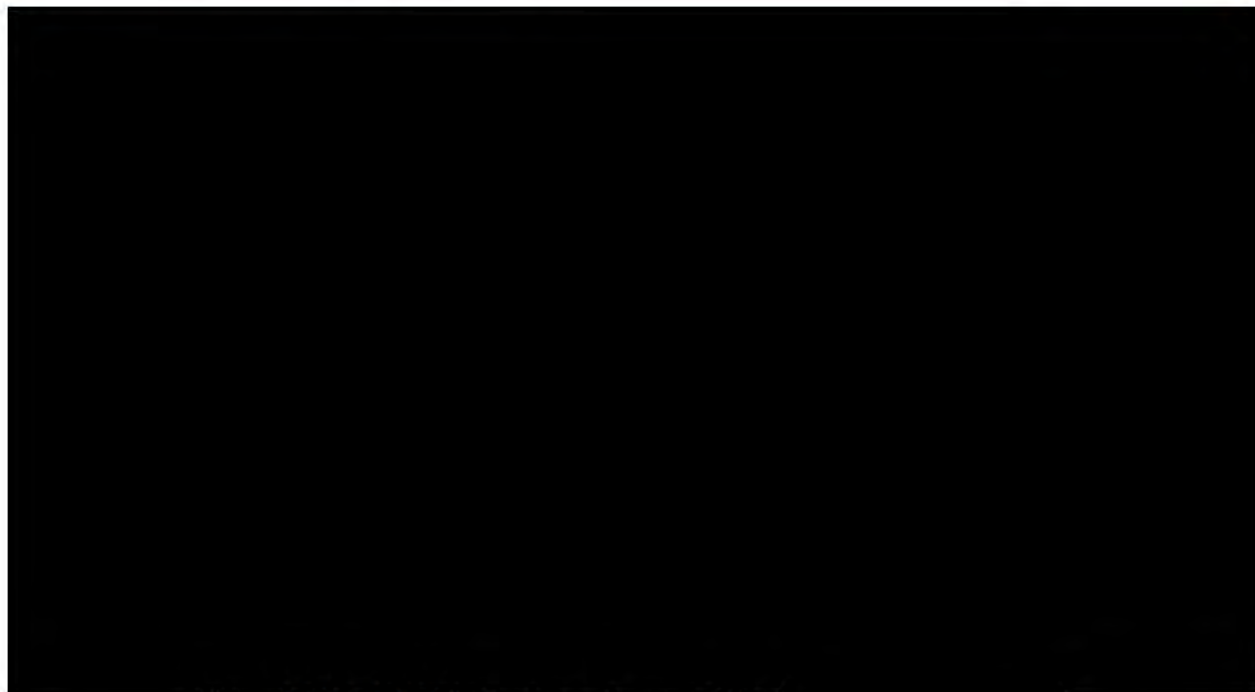


Figure 1.1.4-1. AT&T EIS Customer Support Office.

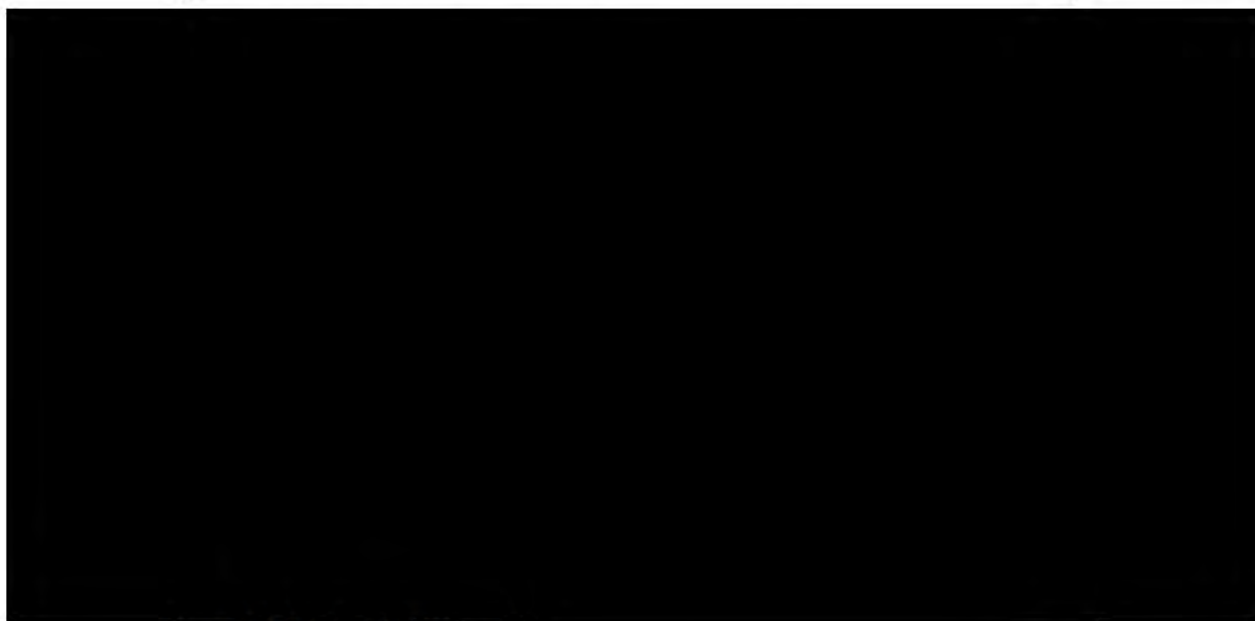


Figure 1.1.4-2. Service Delivery.

Facilitating these requirements is our Business Center portal and BSS shown in the middle. AT&T also provides Client Executive teams that specialize in fully Representatives and are solely focused on their assigned agencies' needs, including requirements planning and billing reconciliation, collaboration tools, and toll-free

number (1-844-EIS-ATT1). Through our Business Center portal, the government can easily access all aspects of their services and gain visibility throughout. By selecting Government Center, the government gains access to our SLA performance data, found under the Service Management option.

Figure 1.1.4-3 illustrates the ease of contacting the AT&T fully integrated EIS CSO.

1.1.4.2 Customer Support Office and Technical Support [G.6.2]

Our existing CSO is located on AT&T premises and supports the government to maximize agency satisfaction with the sales, service and implementation activities on our Networkx contracts. The CSO for EIS will be fully operational within 30 days of the Notice To Proceed (NTP). Upon contract award, primary contact routes such as the main toll-free number and email address will be operational. **Table 1.1.4-1** details the required CSO and technical support functions.



Figure 1.1.4-3. EIS CSO is Easy to Contact. GSA and agencies have 24x7x365 access through a dedicated number or via our highly secure Business Center portal

Table 1.1.4-1. AT&T CSO. Agencies and GSA receive full support and functionality from AT&T's EIS CSO.

CSO Operational Functions
Facilitate the Government's Use of the Contract. [G.6.2(1)]
Provide Contact Information for Each Functional Area of the CSO [G.6.2(2)]
Respond to General Inquiries [G.6.2(3)]
Provide Information Regarding Available Products and Services, Respond to Service Inquiries, And Accept Orders [G.6.2(4)]
Provide Training Registration and Scheduling Information [G.6.2(5)]
Respond to Inquiries Via the Same Method the User Used to Access the CSO, Unless Otherwise Specified by the User [G.6.2(6)]
Provide A Main US Toll-Free Telephone Number Through Which All CSO Functional Areas Can Be Accessed [G.6.2(7)]
Provide the Capability for Non-Domestic Users to Contact the CSO Without Incurring International Charges and Minimize, To the Extent Possible, the Different CSO Contact Numbers Required to Support Non-Domestic Users [G.6.2(8)]
Provide Hot-Links From AT&T's Public EIS Website(S) To CSO Functional Area Email Addresses [G.6.2(9)] www.att.com/gov/eis
Provide Telecommunications Device for the Deaf (TDD) Access to the CSO for Government Representatives Who Are Hearing Impaired or Have Speech Disabilities [G.6.2(10)]
Deal Effectively with the Geographical Distribution of EIS Subscribing Agencies, GSA's Program Management Offices (PMO) In the GSA Regions, And GSA International Activities [G.6.2(11)]
Provide Responses to User Inquiries of A General Nature Such As AT&T's Established Administrative and Operational Procedures, AT&T's Points of Contact, And User forum Information [G.6.2(12)]

CSO Operational Functions
▪ Provide Information on Available Training Classes as Well as Guidance and Assistance with Registration for Training Classes. Training Requirements Are Described in Section 1.1.8 Training [G.6.2(13)] ▪ Provide Technical Support to Agencies and the PMO Regarding the Services AT&T Delivers to the Government [G.6.2(14)]. Technical support includes, but is not limited to: ▪ Answering Questions Related to How Users Can Obtain the Functions Designed into the Services AT&T Provides Via the Contract [G.6.2(14)(a)] ▪ Advising Users on the Capabilities Incorporated into Service Features [G.6.2(14)(b)] ▪ Providing Technical Support to Assist Either AT&T Technicians or the Agencies or Other Organizations or Personnel in the Timely Resolution of Troubles [G.6.2(14)(c)] ▪ Notifying Users of New Services and Features That Are Planned or That Have Recently Been Added to the Contract [G.6.2(14)(d)] ▪ Providing Ordering and Tracking Support Services [G.6.2(14)(e)] ▪ Providing Support to Help Resolve Billing Issues [G.6.2(14)(f)] ▪ Providing Inventory Management Support [G.6.2(14)(g)]

Additionally, **Figure 1.1.4-4** depicts the alignment of our organization to these exact functions.

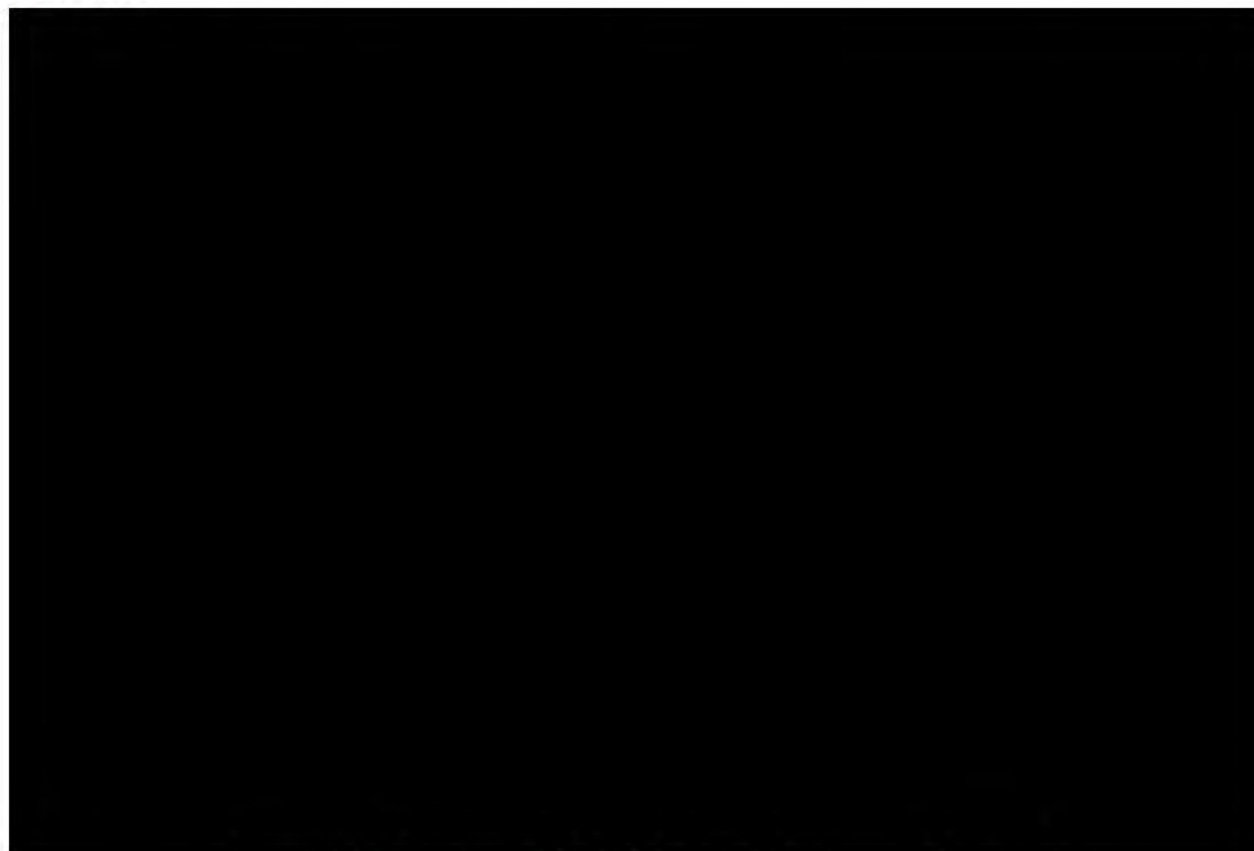


Figure 1.1.4-4. Mapping to GSA CSO Technical Requirements.

The CSO role is discussed in further detail in **Appendix A** and throughout this proposal volume.

1.1.4.3 Supply Chain Risk Management [G.6.3]

AT&T is compliant with SCRM Plan requirements. This plan is discussed in **Appendix B** of this volume and will demonstrate how we reduce and mitigate supply chain risks.

1.1.4.3.1 Plan Submittal and Review [G.6.3.1]

Appendix B is submitted with this proposal volume. AT&T will update and submit the SCRM Plan to the COR and CO annually or as required.

1.1.5 Trouble Ticket Management [L.30.1(1)(a); M.2.2(1 of 3); G.6.4]

GSA and customer agencies will receive quick corrective actions to provide high quality, highly reliable service delivery using AT&T's trouble ticket management processes. As described in **Appendix A, Section A-6**, we apply [REDACTED]

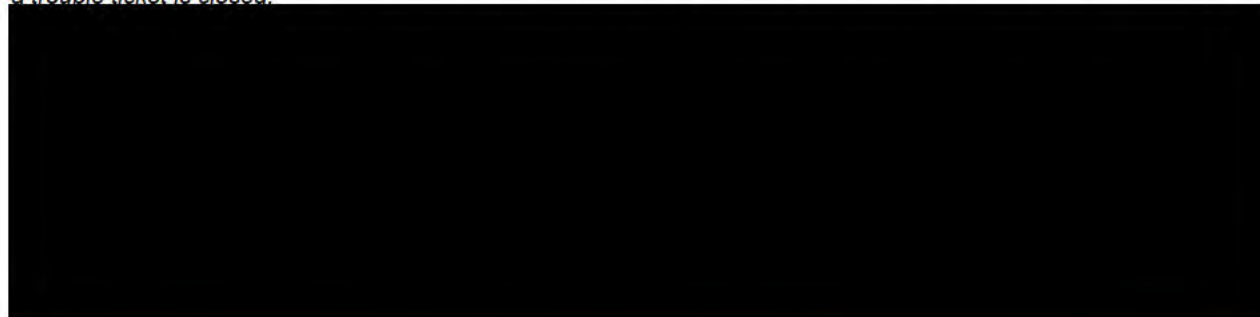
[REDACTED] Our CSO implements procedures and

systems for our
24x7x365 Help Desk to
document and resolve
trouble tickets and for
complaint collection,

Figure 1.1.5-1. AT&T's Trouble Ticket Management. [REDACTED]

entry, tracking, analysis, priority classification, and escalation for all services. The government can call our 24x7 number, 1-844-EIS-ATT1, to open a Trouble Ticket. Once we open a Trouble Ticket and assign it to a member of the Service Assurance team for resolution our objective is to resolve problems within the times specified in EIS RFP Section G.8.2.1.2. **Figure 1.1.5-1** shows our four-step Trouble Ticket Management Process. **Table 1.1.5-1** shows some of the customer services we routinely provide that exceed contract requirements.

Table 1.1.5-1. Our Customer Service. *We continue to provide GSA and agencies with Customer Service even after a trouble ticket is closed.*



Our “Above and Beyond” Customer Service After a Trouble Ticket Has Closed	Benefits to GSA/Agencies

AT&T’s trouble ticket management conforms to commercial best practices and meets the government’s requirements.

1.1.5.1 Trouble Ticket Management General Requirements [G.6.4.1]

Our CSO uses several tools to easily accommodate agency preferences for Trouble Ticket Management tools on a TO basis.

Trouble Ticket Generation: When trouble is detected, GSA and agencies require resolution as quickly as possible. Improperly functioning services can adversely affect mission delivery, citizen services, and other daily operations. To effectively address troubles within the times specified in RFP Section G.8,

When a customer reports a trouble issue or a trouble is detected,

AT&T Offers GSA and Agencies

- High Quality Service
- End-to-end Maintenance Support
- Dedication to Success of Your Critical Missions.

Trouble Ticket Management:



Table 1.1.5-2

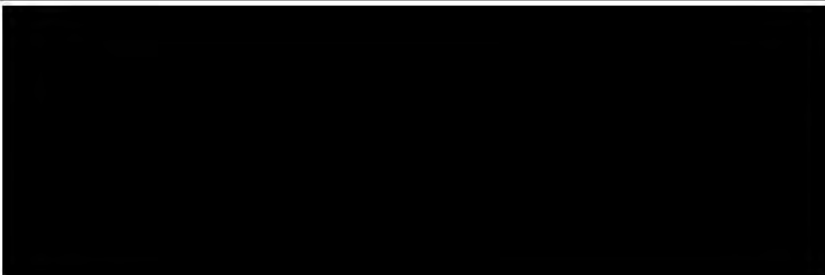
shows the various priority levels and the conditions that lead to their assignment.

Table 1.1.5-2. Trouble Ticket Priorities.

Severity	Priority Type	Priority Definition
Severity 1		
Severity 2		
Severity 3		

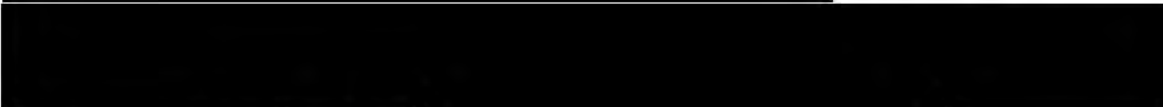


1.1.5.2 Reporting Information [G.6.4.2]



AT&T CSO Assists Agencies

- Analyze SLA Reports
 - Trouble Ticketing
 - Time to Restore
- Calculation Tools
- Enhanced Reports
- Training.



Section 1.1.7

1.1.6 Inventory Management [L.30.1(1)(a); M.2.2(1 of 3); G.7]

GSA and customer agencies will benefit from AT&T's successful 20-year record of accomplishment in inventory management on multiple GSA programs including, maintaining a [REDACTED] inventory accuracy rating on the current Networkx and Enterprise contracts. AT&T understands the criticality of maintaining complete and accurate inventories within the EIS program. Whether transitioning new agencies onto the EIS program or supporting technology refresh initiatives from existing agencies, the accuracy of inventories maintained is essential to managing network and service configurations throughout the entire period of performance. AT&T's experience gained in inventory management as a prime contractor on the current Networkx contracts includes managing an inventory exceeding [REDACTED]

[REDACTED] This functional and systems skill is easily migrated to support the EIS requirements. The overall capabilities derived from our past experience are summarized in **Table 1.1.6-1**.

Did You Know?

AT&T is successfully managing over [REDACTED] inventory records for [REDACTED] agencies on Networkx.

Table 1.1.6-1. Inventory Management Features and Benefits.

AT&T Features	GSA and Agency Benefits
[REDACTED]	[REDACTED]

AT&T Features	GSA and Agency Benefits

1.1.6.1 Inventory Management Process Definition [G.7.1]

Access to timely and accurate inventory information is critical to efficient management of the government's EIS services. As new or enhanced services are added AT&T will support additional inventory data elements. The GSA and subscribing agencies are provided complete and accurate EIS inventory data using highly

Figure 1.1.6-1, and discussed in RFP Section G.5.3.1.

the government can view
accurate and current inventory
data, make queries, obtain
reports, verify billing, and
perform periodic downloads for
auditing purposes. Agencies
with multiple and complex
requirements can obtain their inventory

Figure 1.1.6-1. AT&T's Government Center Web-Based Access to Inventory Management Functions.

Consequently, the government effectively accesses and manages the EIS inventory

AT&T supports all key inventory management tasks as listed in RFP Section G.7.1. Inventory management requirements associated with transition on or off EIS are discussed in **Appendix A, Section A-2.3**.

Shown in **Figure 1.1.6-2**,

Section 1.1.6.1.4.

1.1.6.1.1 Inventory Management Functional Requirements [G.7.1.1]

AT&T populates the EIS Inventory database with fields from the SOCN such as the AHC, UBI, and CLIN. Within each of the IR requirements, [REDACTED]

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



Figure 1.1.6-2. Key Inventory Management Tasks.

All EIS services are maintained and [REDACTED]

[REDACTED] within one business day of the issuance of the SOCN. Updates include all additions, deletions or changes to the EIS services being provided to GSA and agencies.

Procedurally, the government will electronically receive a SOCN. All the data elements listed on the SOCN are maintained and updated, as required, in the [REDACTED]

As services are delivered to and accepted by the government, a SOCN is available to the GSA and the ordering Customer Agency. The data elements are listed on the SOCN and in the EIS Inventory database as applicable for each EIS service provided. [REDACTED]

[REDACTED] In cases of administrative order changes where a SOCN is not required, we will submit a SOAC to update the inventory management database.

Updates to the inventory are driven by service orders. Therefore, changes to the service, such as added features, replacement of SRE, or disconnects, are recorded in the [REDACTED] as indicated by the data in the SOCN for that service order. If incorrect inventory data is identified and resolved, later corrections to the inventory will be initiated through a special records order. The resulting SOCN will indicate that the corrected changes have been processed as a resolution to an inventory data discrepancy.

[REDACTED]

[REDACTED] Section 1.1.1.

The government's complex task of accounting for a large number of products and services is made easier [REDACTED] GSA and subscribing agencies can be confident that their information is current, accurate, secured, and easily accessible for billing and IR.

1.1.6.1.1 Fully Populate the EIS Inventory with the Data Elements of the IR As Defined in Section J.2.7 Inventory Management [G.7.1.1(1)]

[REDACTED] is fully populated with all the data elements of the IR (i.e., agency_hierarchy_code, contract_line_item_number, and unique_billing_identifier) as contained within the SOCN data elements shown in **Table 1.1.6-2**.

Table 1.1.6-2. SOCN Data Elements. [REDACTED]

Data Element Field Name	Description
agency_hierarchy_code	An internal government accounting code that must be tracked for all services from order submission through disconnection
agency_order_sent_date	Date that order was sent by agency
agency_task_order_num	Agency TO number; also known as the Procurement Instrument Identifier (PIID).
base_line_item_price	Base price amount of the line item without the AGF
charging_frequency_and_sre_element_code	Charge frequency description (e.g., Monthly Recurring Charges (MRC), NRC, Usage, and SRE Pricing Element etc.) Code

Data Element Field Name	Description
charging_unit_code	Code defining the specific charge unit (e.g., per port, per time-increment, etc.)
clin_description	CLINs Description
contract_line_item_number	CLINs. Used to uniquely identify services available on the contract. Agency or AT&T may provide CLINs; all CLINs must be approved via an order by the agency before the activity starts.
contract_number	EIS contract number assigned to AT&T (Not the TO number)
contracting_officer_representative_email_address	COR email address
contractor_invoice_level_account_number	
contractor_service_level_account_number	
contractor_service_request_number	
data_transaction_code	Identifies the transaction represented by the file or data exchange
data_transaction_file_date	Submission date for the data set
data_transaction_sequence_num	Uniquely identifies each data exchange transaction. If it becomes necessary to examine a transaction in detail, this number will ensure that all parties are referring to the same transaction. Other than the data type and length, the submitting party is free to create this number in any manner desired (e.g., a millisecond-level timestamp based on data submission time)
early_installation_code	Indicates whether an agency will accept services before contractual due date
fully_loaded_price_code	
iconectiv_nsc	iconectiv Network Site Code for the originating location (Service Delivery Address)
location_city	City for this order location (Service Delivery Address)
location_country	Country for this order location (Service Delivery Address)
location_postal_code	Postal code for this order location (Service Delivery Address)
non-recurring_charge_waiver_code	Non-Recurring Charge (NRC) waiver - Yes or No
order_header_type_code	Indicates the overall order type
order_item_type_code	Indicates the order type for this line item
order_method_code	
originating_jurisdiction_code	Applies to domestic Continental United States/Outside Contiguous United States (CONUS/OCONUS) or non-domestic
quantity	Numeric count for the item specified by the CLIN
Unit Price	Price of Ordered component
service_order_completion_date	Date service was completed
street_name	The street name of the address (Service Delivery Address)
street_number	The street number of the address (Service Delivery Address)

Data Element Field Name	Description
ubi_state	The current service state of the UBI. Options are: Active = The UBI is active with charges accumulating Inactive = The UBI is inactive with no charges accumulating Band_Name = The band-priced UBI is in the band listed. Note: the state is the actual band name/designator as defined in RFP Section B and/or the TO
unique_billing_identifier	Uniquely identifies one or more items linked together for ordering, billing and inventory management purposes

1.1.6.1.1.2 Initially Populate Records of EIS Services in the EIS Inventory Within One (1) Business Day of the Issuance of SOCNS for EIS Services Delivered to Customers [G.7.1.1(2)]

All services ordered and provisioned will be populated in our [REDACTED]

[REDACTED] within one business day of the SOCN. [REDACTED]

As a service order is completed, [REDACTED]

[REDACTED] Table 1.1.6-3 consolidates our response to those RFP requirements defined in RFP Section G.7.1.1.2.

Table 1.1.6-3. Inventory Management Functional Requirements. [REDACTED]

RFP Requirement	AT&T Response
Establish an Inventory for All EIS Services Provided to Its Customers [G.7.1.1(2)(a)]	Sections 1.1.6.1.1 and 1.1.6.1.1.1. [REDACTED]
Maintain and Update the EIS Inventory for All EIS Services Provided to Its Customers [G.7.1.1(2)(b)]	Section 1.1.1. Table 1.1.6-2. [REDACTED]
Make the EIS Inventory Data Available to the Government [G.7.1.1(2)(c)]	[REDACTED]

1.1.6.1.1.3 Deliver IR Deliverable Each Month as Defined in Section J.2.7 Inventory Management [G.7.1.1(3)]

AT&T will comply with the RFP requirements for EIS and provide the IR deliverable by the 15th day each month, and will comply with the transfer mechanisms defined in RFP Section J.2.7 including Secure FTP, email (if requested by the government), [REDACTED] or other means as agreed to. Additional information related to data transfer formats can be found in **Section 1.1.3.2.2.2**.

1.1.6.1.2 EIS Inventory Maintenance [G.7.1.2]

Requirements for maintaining the inventory and implementing updates to inventory services within one business day have been previously discussed in **Section 1.1.6.1.1.2**.

1.1.6.1.3 EIS Inventory Data Availability [G.7.1.3]

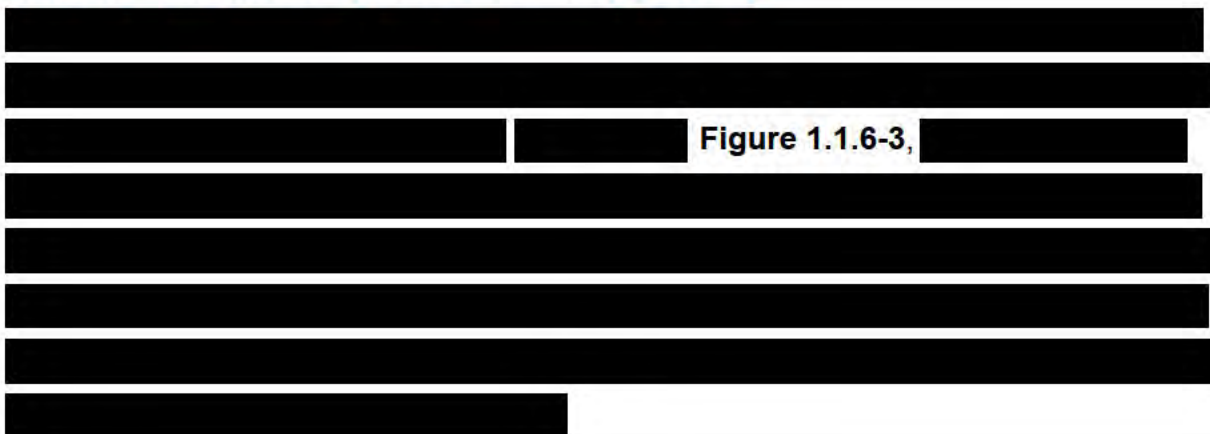


Figure 1.1.6-3. EIS Data Availability for Government Customers.

Older monthly snapshots that have been archived will be available for self-service query through the [REDACTED] within five days of when a government customer requests them. Archived EIS monthly snapshots are retained and when requested, unrestricted access will be provided to authorized government customers during the contract and for three years following the expiration or termination of the

contract. Access security and performance requirements specified in RFP Section G.5.6 are supported [REDACTED]

When the government requests either in entirety or for a subset, [REDACTED]

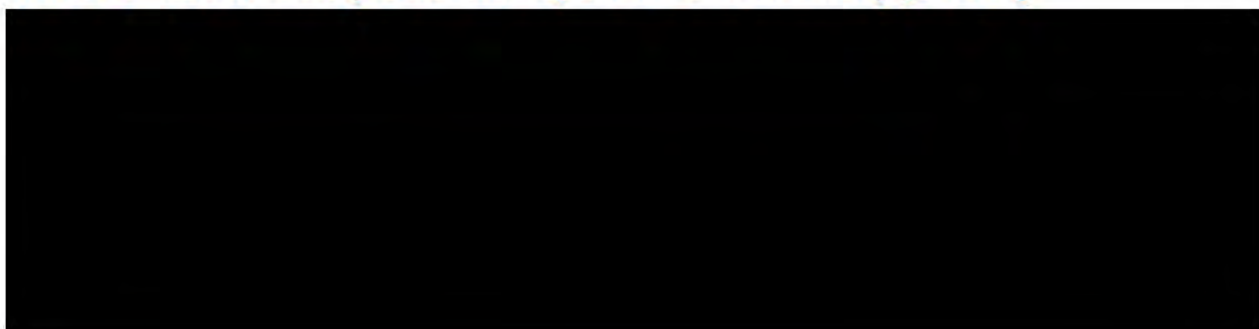
(see Table 1.1.6-4).

Table 1.1.6-4. Inventory Data Availability. *AT&T's Inventory Management system provides highly secure electronic access, standard industry formats, and monthly snapshots within the 5-day timeframe allotted by GSA.*

AT&T Proposal Section/RFP Requirement	AT&T Proposal Response
Provide to Government Users Secure Electronic Access to the Current View and To the Monthly Snapshots of EIS Services in the Contractor-Maintained EIS Inventory [G.7.1.3(1)]	[REDACTED]
For Secure Web-Based Queries Against the Contractor-Maintained EIS Inventory [G.7.1.3(2)]	[REDACTED]
Provide Government Users the Option to Select A User Choice of Online Viewing, Data File Downloading [G.7.1.3(2)(a)]	[REDACTED]
Provide and Maintain on Its EIS BSS Web Interface A Link for Secure, Electronic Access to the Contractor-Maintained EIS Inventory Information [G.7.1.3(2)(b)]	[REDACTED]
For Data Export or Data File Delivery in Response to A Secure Query Against the Contractor-Maintained EIS Inventory [G.7.1.3(3)]	[REDACTED]
Support Common Industry Standard Formats and File Structures [G.7.1.3(3)(a)]	[REDACTED]
Impose No Limit on the Number of Records That Is Less Than the Limit	[REDACTED]

AT&T Proposal Section/RFP Requirement	AT&T Proposal Response
Imposed by the File format Specification [G.7.1.3(3)(b)]	
Make Older Monthly Snapshots of the EIS Inventory That Have Been Archived Available for Query Access, Within Five (5) Days of A Government Request [G.7.1.3(4)]	
Retain the Monthly Snapshots of the EIS Inventory and Provide them To the Government as Requested for Three (3) Years Following the Expiration or Termination of the Contract [G.7.1.3(5)]	
Meet or Exceed the Access Security and Performance Requirements Specified in RFP Section G.5.6. BSS Security Requirements for the System Used for the EIS Inventory [G.7.1.3(6)]	
Provide A Copy Of the Records, In the format Requested By the Government, With Data Field Labels, In the Current EIS Inventory Or Any Of the Monthly Snapshots Either In their Entirety Or for A Subset Specified In the Government's Request [G.7.1.3(7)]	
Provide A Copy of the Records in the Current EIS Inventory, In the format Requested by the Government, in their Entirety of for A Subset Specified in the Government's Request [G.7.1.3(8)]	
Not Restrict the Use by the Government of Any and All EIS Inventory Data Related to This Contract During the Contract and for Three (3) Years Following the Expiration or Termination of the Contract [G.7.1.3(9)]	

1.1.6.1.4 EIS Inventory Data Discrepancies and Accuracy [G.7.1.4]



[REDACTED]

The [REDACTED] This

information is submitted with each discrepancy, [REDACTED]
Each stakeholder can view a status for the

[REDACTED]

Figure 1.1.6-4. [REDACTED]

[REDACTED]

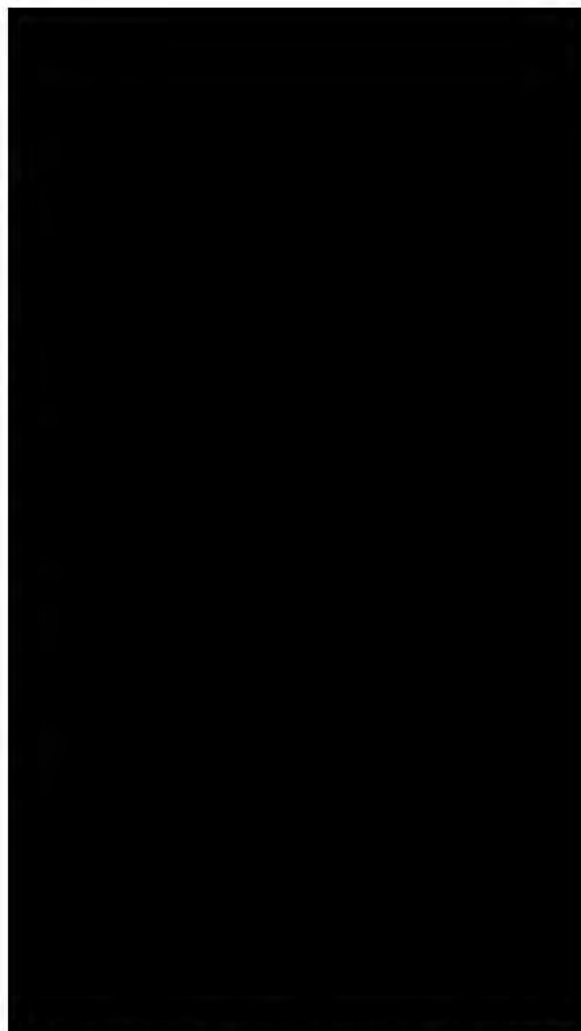


Figure 1.1.6-4. Inventory Discrepancy Handling Process Flowchart. *AT&T involves all stakeholders to make sure discrepancy issues are properly resolved.*

[REDACTED] a SOCN is established and signifies that the correction has been completed.

1.1.6.1.4.1 Inventory Data Discrepancies [G.7.1.4.1]

EIS inventory discrepancy notifications reported by the government will be reviewed and assessed promptly. [REDACTED]

[REDACTED] the agency's concerns they may issue a formal inventory dispute as indicate in RFP Section J.2.6.1. [REDACTED]

1.1.6.1.4.2 EIS Inventory Data Accuracy [G.7.1.4.2]

[REDACTED] **Figure 1.1.6-5.** These are designed to verify EIS inventory is complete and correct. In addition, if EIS inventory data discrepancy occurs because of missing or incomplete data elements in the SOCN or Billing Detail (BD), actions will be taken to correct these discrepancies.

Figure 1.1.6-5. AT&T Internal Audits.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] All data discrepancies that are identified, [REDACTED], will be reconciled within 10 days of notification.

1.1.6.1.5 EIS Inventory Reconciliation [G.7.1.5]

An Inventory Reconciliation Report is provided to GSA for review by the 15th of each month. [REDACTED]

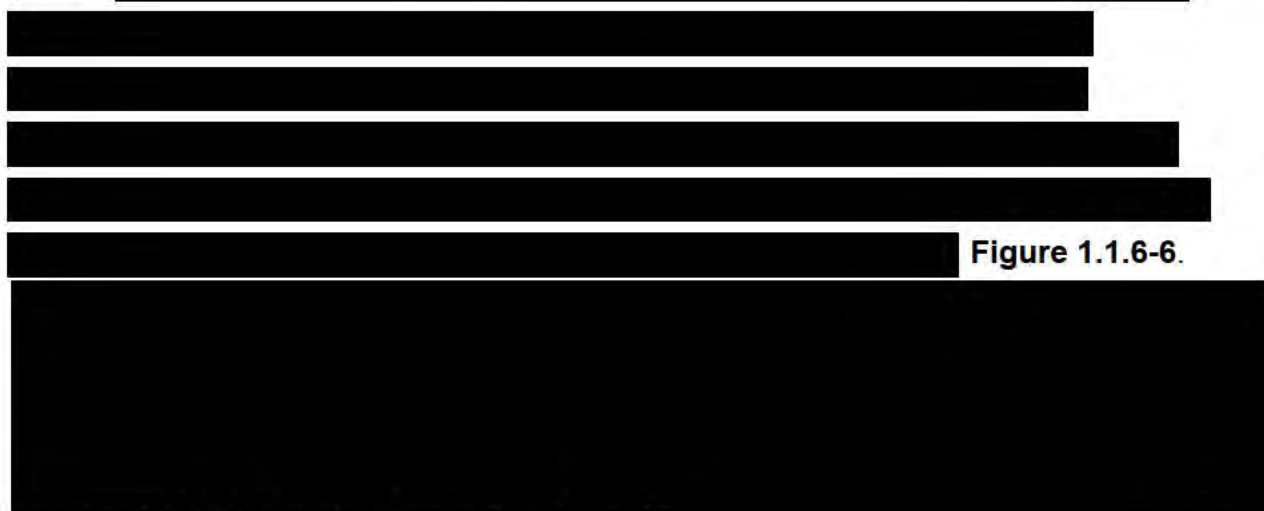


Figure 1.1.6-6. EIS Inventory Reconciliation Report.

1.1.7 Service Level Management [L.30.1(1)(a); M.2.2(1 of 3); G.8]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1.1.7.1 Overview [G.8.1]

An SLA is an agreement between the government and AT&T to provide a service at a performance level that meets or exceeds performance objective(s) specified by the government in the contract. The EIS contract and its SLAs have specific KPIs for nearly all services.

If AT&T offers a service, we comply with the associated KPIs and AQLs. Certain services deemed essential to government operations require mandatory SLAs.

Our CSO's [REDACTED] (Figure 1.1.7-1) [REDACTED]

Figure 1.1.7-1. AT&T Organization for SLA Management.

Our processes are forward looking in addition to managing current performance to maximum efficiency and effectiveness; we use our ongoing analysis of service and SLA performance as the basis for continuous improvement of all our services. If the specified service levels are not met, AT&T responds to government credit requests issued through the SLACR process. As needed, AT&T issues credits per formulas set up for each type of SLA.

1.1.7.2 Service Level Agreement Tables [G.8.2]

If AT&T offers a service, or if a service is included with standard SLAs on a TO, the following SLAs will apply: Service Performance SLAs, Service Provisioning SLAs, and Billing Accuracy SLA. [REDACTED]

AT&T understands that the SLAs in this document represent a minimum level of service acceptable to the government unless otherwise specified in a TO. Agencies may define additional or different SLAs, KPIs and AQLs during the TO process. These TO-specific SLAs are equally binding, [REDACTED]

[REDACTED] The government considers the service specific SLA table and associated references to be its Quality Assurance Plan; [REDACTED]

1.1.7.2.1 Service Performance SLAs [G.8.2.1]

Service performance SLAs measure how well services are performed. They include: Service-Specific SLAs, Incident Based Service SLAs, and Service Related Labor SLAs.

Table 1.1.7-1 describes AT&T's approach to service specific SLAs in more detail.

Table 1.1.7-1. Service Performance SLAs [G.8.2.1]. AT&T intensively manages our performance on Service Performance SLAs to meet or exceed the KPIs and AQLs.

SLA Type	Description
Service-Specific SLAs [G.8.2.1.1]	Service-specific SLAs are performance measures demonstrating the overall performance of a single TO service.
	Service-Specific SLA Table [G.8.2.1.1.1] - Virtual Private Network Service (VPNS) [C.2.1.1.4] - Ethernet Service [C.2.1.2.4] - Optical Wavelength Service [C.2.1.3.4] - Private Line Service [C.2.1.4.4] - Synchronized Optical Network Service [C.2.1.5.4] - Dark Fiber Service [C.2.1.6.4] - Internet Protocol Service [C.2.1.7.4] - Internet Protocol Voice Service [C.2.2.1.4] - Toll Free Service [C.2.2.3.4] - Contact Center Service [C.2.3.1.7] - Collocated Hosting Center Service [C.2.4.5.1] - Content Delivery Network Service [C.2.5.4.4]
	- Wireless Service [C.2.6.4.1] - Managed Network Service [C.2.8.1.4] - Web Conferencing Service [C.2.8.2.4] - Unified Communications Service [C.2.8.3.4] - Managed Trusted Internet Protocol Service (MTIPS) [C.2.8.4.4] — Trusted Internet Connection (TIC) portal [C.2.8.4.4.1] - MTIPS — Transport Collection and Distribution [C.2.8.4.4.2] - Managed Security Service [C.2.8.5.4] - Managed Mobility Service [C.2.8.6.5] - Audio Conferencing Service (ACS) [C.2.8.7.4] - DHS Intrusion Prevention Security Service [C.2.8.9.4]
	Service-Specific SLA Credit formulas [G.8.2.1.1.2]

SLA Type	Description
Incident-Based Service SLAs [G.8.2.1.2]	The Time to Restore (TTR) SLA Failure to meet the AQL for an individual incident constitutes failing the SLA for that incident unless due to documented delays caused by the customer. Incident-Based Service SLA References [G.8.2.1.2.1] - Virtual Private Network Service [C.2.1.1.4] - Ethernet Service [C.2.1.2.4] - Optical Wavelength Service [C.2.1.3.4] - Private Line Service [C.2.1.4.4] - Synchronized Optical Network Service [C.2.1.5.4] - Dark Fiber Service [C.2.1.6.4] - Internet Protocol Service [C.2.1.7.4] - Internet Protocol Voice Service [C.2.2.1.4] - Toll Free Service [C.2.2.3.4]; - Contact Center Service [C.2.3.1.7]; - Colocated Hosting Center Service [C.2.4.5.1] - Content Delivery Network Service [C.2.5.4.4] - Wireless Service [C.2.6.4.1] - Commercial Fixed Satellite Service [C.2.7.3] - Managed Network Service [C.2.8.1.4] - Web Conferencing Service [C.2.8.2.4] - Unified Communications Service [C.2.8.3.4] - MTIPS C.2.8.4.4 — Trusted Internet Connection Portal [C.2.8.4.4.1] - MTIPS — Transport Collection and Distribution [C.2.8.4.4.2] - Managed Security Service [C.2.8.5.4] - Managed Mobility Service [C.2.8.6.5] - Audio Conferencing Service [C.2.8.7.4] - Video Teleconferencing Service [C.2.8.8.4] - DHS Intrusion Prevention Security Service [C.2.8.9.4]. Incident-Based Service SLA Credit formula [G.8.2.1.2.2]

SLA Type	Description
Service-Related Labor SLAs [G.8.2.1.3]	

1.1.7.2.2 Service Provisioning SLAs [G.8.2.2]

As described in RFP Section G.3.3.1.3,

Table 1.1.7-2 provides greater detail on credit formula calculation for the three categories of service provisioning SLAs.

Table 1.1.7-2. Service Provisioning SLAs [G.8.2.2]. GSA and agencies receive service dependability through our adherence to Standard Provisioning SLAs.

SLA Type	Description																
Standard Provisioning SLAs [G.8.2.2.1]	Table 1.1.7-3. Standard Service Provisioning Intervals [G.8.2.2.1.1] <table> <tr> <th>Service</th><th>Orders SLA (Days)</th></tr> <tr> <td>Disconnect (all services)</td><td>30</td></tr> <tr> <td>Toll-Free Service (TFS)</td><td>45</td></tr> <tr> <td>Private Line Service (PLS):</td><td></td></tr> <tr> <td>• PLS ≤ Digital Signal 1 (DS1)</td><td>45</td></tr> <tr> <td>• DS1 < PLS ≤ DS3</td><td>85</td></tr> <tr> <td>• DS3 < PLS ≤ Optical Carrier 3 (OC3)</td><td>120</td></tr> <tr> <td>Virtual Private Network Service</td><td>45</td></tr> </table>	Service	Orders SLA (Days)	Disconnect (all services)	30	Toll-Free Service (TFS)	45	Private Line Service (PLS):		• PLS ≤ Digital Signal 1 (DS1)	45	• DS1 < PLS ≤ DS3	85	• DS3 < PLS ≤ Optical Carrier 3 (OC3)	120	Virtual Private Network Service	45
Service	Orders SLA (Days)																
Disconnect (all services)	30																
Toll-Free Service (TFS)	45																
Private Line Service (PLS):																	
• PLS ≤ Digital Signal 1 (DS1)	45																
• DS1 < PLS ≤ DS3	85																
• DS3 < PLS ≤ Optical Carrier 3 (OC3)	120																
Virtual Private Network Service	45																
Individual Case Basis Provisioning SLAs [G.8.2.2.2]	Services Subject to ICB Provisioning Intervals [G.8.2.2.2.1] - Audio Conferencing Service - Managed Network Service - Managed Security Service - Cloud Infrastructure as a Service - MTIPS																

SLA Type	Description
	- Managed Mobility Service - Optical Wavelength Service - Unified Communications Service - Voice Services - Web Conferencing Service.
Project Provisioning SLAs [G.8.2.2.3]	- Cloud Content Delivery Network Service - Collocated Hosting Service - Commercial Fixed Satellite Services - Contact Center Service - Dark Fiber Service - Ethernet Service - Internet Protocol Service
	Section G.8.2.2.

Rapidly Provisioned Services [G.8.2.2.4] are also subject to service provisioning SLAs however, the calculations may be different. As telecommunication services evolve, provisioning become faster, and for many services, agencies “provision” the services themselves. These services lend themselves to rapid provisioning, which streamlines the provisioning process and only requires the SOA and SOCN. Services are subject to rapid provisioning if all of the following conditions apply:

- The provisioning interval shall not exceed 48 continuous hours.
- The proposed provisioning interval shall be used to calculate SLA compliance as described in Section G.8.2.2.
- Any CWD (see Section G.3.3.1.3) specified in the order does not apply, and early installation is acceptable.

The bandwidth increments and decrements on demand are a rapidly provisioned service and follow the requirements described in G.3.3.3.2 Rapid Provisioning Orders.

Table 1.1.7-4. Rapidly Provisioned Services [G.8.2.2.4]. GSA and agencies benefit from the self-provisioned and rapidly provisioned services offered by AT&T.

SLA Type	Description
Cloud Service Provisioning [G.8.2.2.4.1]	Within the criteria of rapid and elastic provisioning for cloud services as defined by NIST, and as referenced in RFP Section C.2.5, AT&T's offered Cloud services include Infrastructure as a Service and Platform as a Service which includes a standard-provisioned account set-up CLIN and numerous self-provisioned Cloud Infrastructure element CLINs. The SOCN notice for the account set-up CLIN will include all of the auto-sold/self-provisioned Infrastructure element CLINs. The account set-up CLIN follows the standard tracking of the ordering, confirmation, and provisioning intervals (e.g. SOA/SOC/FOCN/SOCN). The self-provisioning portal allows electronic tracking of the ordering, confirmation, and provisioning of the Cloud

SLA Type	Description				
	Infrastructure elements. The intervals for both the standard set-up CLIN and the auto-sold/self-provisioned CLINs can be accurately tracked as described in RFP Section G.3.3.3.2. AT&T proposes the following cloud-provisioning intervals: - Initial account set-up: 48 hours - Self-provisioned IaaS CLINs (new, delete, change): monthly virtual server instance provisioning in 15 minutes and monthly physical server provisioning in 48 continuous hours. - Self-provisioned PaaS CLINs (new, delete, change): virtual database instance provisioning in 15 minutes. - Disconnect of entire account: 5 business days. - All CLINs in support of Software as a Service are subject to the 48-hour interval.				
Bandwidth-on-Demand [G.8.2.2.4.2]	As described in RFP Section C.2.1.2, AT&T supports bandwidth increments and decrements on demand, as agreed between AT&T and the agency. Unless otherwise agreed by the agency and AT&T on a case-by-case basis, provisioning time for this feature will meet the following standard shown in Table 1.1.7-5, measured from the service order to the SOCN. Table 1.1.7-5. Standard Service Provisioning Intervals [G.8.2.2.1.1] <table> <tr> <th>Service</th><th>Provisioning SLA</th></tr> <tr> <td>Ethernet Services: Bandwidth-on-Demand Changes</td><td>24 Hours</td></tr> </table>	Service	Provisioning SLA	Ethernet Services: Bandwidth-on-Demand Changes	24 Hours
Service	Provisioning SLA				
Ethernet Services: Bandwidth-on-Demand Changes	24 Hours				

Service Provisioning SLA Credit Formulas [G.8.2.2.5]: AT&T will apply associated credits in accordance with RFP Section G.8.4 for each failed SLA. This provisioning credit is the largest of 50% of the non-recurring charge or 50% of the MRC.

1.1.7.2.3 Billing Accuracy SLA [G.8.2.3]

1.1.7.3 Service Level General Requirements [G.8.3]

1.1.7.3.1 Measurement [G.8.3.1]

Section A-6

1.1.7.3.2 Reporting [G.8.3.2]

[REDACTED]

Section 1.1.7.5.

1.1.7.3.3 Credits and Adjustments [G.8.3.3]

[REDACTED]

[REDACTED]

1.1.7.4 SLA Credit Management Methodology [G.8.4]

[REDACTED]

[REDACTED]

[REDACTED] RFP Section

G.8.2. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1.1.7.4.1 Credit Management [G.8.4.1]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] RFP Section

G.4.4.

1.1.7.5 Service Level Reporting Requirements [G.8.5]

1.1.7.5.1 Report Submission [G.8.5.1]

[REDACTED]

Table 1.1.7-6. [REDACTED]

[REDACTED]

[REDACTED]

1.1.7.5.2 Report Definitions [G.8.5.2]

Table 1.1.7-6 provides details of the content of AT&T's SLA reports.

Table 1.1.7-6. Report Definitions.

Report Type	Definition
Service Level Agreement Report [G.8.5.2.1]	
SLA Credit Request (SLACR) Response [G.8.5.2.2]	
Trouble Management Performance Summary Report [G.8.5.2.3]	
Trouble Management Incident Performance Report [G.8.5.2.4]	

1.1.8 Training [L.30.1(1)(a); M.2.2(1 of 3); G.10(1-6)]

GSA and customer agencies will receive effective, accurate, and timely EIS training and courseware that is updated to keep up with changes during the life of the contract. GSA and agencies can take

advantage of AT&T's robust EIS training program, which we designed to address the diverse needs of GSA and EIS customers. AT&T's training program provides a high-quality, flexible, and easily accessible learning experience as part of the basic service, at no additional charge to the government, throughout the life of AT&T's EIS

contract. Our EIS training program includes courseware development, evaluation, continuous improvement and a variety of delivery methods, including classroom instructors when required/requested. AT&T supports

additional (specialized) training required by TOs when requested by an agency.

Experienced AT&T Training professionals offer government users the expertise required to successfully obtain and manage AT&T's EIS services.

A dedicated EIS Training Manager and staff, provided by the AT&T CSO, lead support for government EIS training. This team is fully accountable for meeting all training

requirements, including, course design and development, delivery, and ongoing updates based on student feedback and technology changes. In addition, the CSO assists users experiencing difficulties and provides training as required through continuous monitoring and analysis of the EIS training program.

AT&T's commitment to the highest quality of service for our customers includes mandatory onboard training for AT&T employees and contractor staff engaged in providing EIS services to our customers. In addition all AT&T personnel are required to fully review and acknowledge the AT&T Code of Business Conduct as well as the Corporate Personal Integrity Plan (C/PIP), which outlines how AT&T personnel should interact with Federal employees with respect to gifts, gratuities and entertainment as well as procurement integrity.

1.1.8.1 Draft Customer Training Plan [G.10; F.2.1]

This draft training plan meets all of the government requirements listed in RFP Section G.10. The government may provide comments within 30 days of NTP. After comments are received, AT&T will incorporate GSA comments and revisions and will deliver the revised training Plan within 15 days after receipt of comments.

The AT&T EIS training program will deliver training and education to government customers on all aspects of the contract including timely topical overviews, BSS, processes and procedures, transition activities and security management. We deliver training to government audiences through a variety of flexible training methods shown in **Figure 1.1.8-1**.

AT&T employs Networkx proven instructional development and design processes to create training content and materials to meet the unique needs of the EIS program. Each course is validated to meet industry accepted quality control processes. The AT&T EIS training program also features the ability to provide training through multiple delivery methods based on course content, customer requests, student population, logistics, and deployment schedules. We will use lessons learned disciplines from the training currently offered in the Networkx contract to provide continuous assessment and feedback and make the program fully effective and up-to-date.

AT&T modularizes EIS training as much as possible to allow for maximum student flexibility. Students may move from module to module and learn about different topics as they see fit. The basic idea of modularity is that at all levels there is an opportunity to *choose* and *combine* modules in different ways according to the context of each particular teaching situation. For example, students not requiring training on SLA reports can elect to skip that class or module.

AT&T will coordinate with the government in providing training facilities, equipment, and any environmental requirements as needed. If provided by AT&T, training locations will be within daily commuting distance for the government students and will provide appropriate classroom

environment and necessary equipment and support. Delivery formats include formal classroom training, distance learning, web-based training, other remote training methodologies and other methods specified by the government. AT&T will provide training as requested by the government throughout the life of the contract.

1.1.8.1.1 Training Curriculum [G.10.1]

Table 1.1.8-1 provides details of training modules available for AT&T's EIS customers. All courses and modules are available in a variety of delivery methods, and our training staff is prepared to work with agencies to further tailor the courses and modules to specific needs. AT&T also offers an EIS overview module specifically designed for senior executives.



Figure 1.1.8-1. AT&T Training Approach. Government customers have access to a powerful set of learning resources specifically created by AT&T to fully support all aspects of the EIS contract.

Table 1.1.8-1. AT&T's Training Curriculum. *EIS users quickly and effectively learn to initiate and manage their use of EIS services. Modular design and continuous updates allow tailoring of training to meet specific user needs.*

EIS Training Curriculum Matrix			
Course Name (Modules)	Key Topics		General Course Description
EIS Overview and Transition (Module 1) 1 Hour	- Preparation Activities - Timeframes/Intervals - Project Management - EIS Products/Services - EIS Service Features - Government Roles & Responsibilities.		Students receive an end-to-end overview of EIS transition processes/activities, service offerings, features, and benefits.
EIS Ordering (Module 2) 2.0 Hours	- Use Of AT&T's BSS [G.10.1(1)] - Obtaining Price Quotes for Services and Features [G.10.1(2)] - Ordering Services From AT&T Via CLINS or Individual Case Basis(s) (ICBS) [G.10.1(3)] - Submit Service Orders - Track Order Status - Placing Order Electronically to Add, Change, Cancel, Or Disconnect Services [G.10.1(4)] - Adding or Changing the Features, Calling Privileges, Telephone Number or Other Line Attributes That Can Be Changed Via "Soft" Reconfigurations [G.10.1(5)] - Accepting or Rejecting an Order or Part of An Order [G.10.1(6)] - Add/Modify/Delete - View Confirmation Notices.		Government users receive training on all aspects of EIS ordering — for both online and manual processes. Gain a clear understanding of completion notices/confirmations, intervals, modifying or expediting orders, and run EIS price quotes. Learn how to submit changes for calling privileges, telephone number, features and other line attributes via "soft" reconfigurations.
EIS Billing & Billing Dispute (Module 3) 2.0 Hours	- AT&T BSS Portal (billing/bill dispute tools) - Reconciling Billing [G.10.1(7)] - Initiating and Tracking Billing Disputes [G.10.1(8)] - Submit Billing Disputes (G.10.1(8)) - Track Dispute Status [G.10.1(8)] - Initiating the Inventory Management Process [G.10.1(9)] - Billing Adjustments - Coordinate with CSO - Escalate for Resolution - Fraud Prevention - Billing Hierarchies.		A comprehensive course that provides students with a complete view of EIS billing operations. Students learn how to access and analyze bills, submit and manage billing disputes, and escalate or coordinate with the AT&T CSO as required.
EIS Trouble Reports Handling (Module 4) 2.1 Hours	- Initiating and Reconciling Performance Management (SLA) Reports [G.10.1(10)] - View/Obtain Ticket Status - Escalation Procedures - Obtain Credit Adjustments - Submit Complaints - Fraud Prevention. - Placing and Tracking Trouble Reports for Routine and Emergency Troubles [G.10.1(11)]		Detailed course covering the reporting and management of EIS troubles and complaints associated with the operation of EIS services. Students learn how to create, submit, and monitor trouble tickets to full resolution and how to escalate to CSO as required.
Network Management & Monitoring (Module 5)			Primarily an overview for customers with responsibility for managing and monitoring agency networks. Students are able to use network management tools to help promote peak performance and utilization and receive early warning data on service affecting events.

1.1.8.1.2 Training Evaluation [G.10.2]

AT&T evaluates training activities to measure the effect of individual courses and the overall success of the AT&T EIS training program. Internal quality checks and balances are embedded into the design, development, and delivery processes to provide government students with reliable and operational training content and delivery.

Training delivered to the government is evaluated by every student — after every class. The evaluation addresses the instructor, effectiveness, course objectives and applicability of the course material, and training facilities/method, and allows written comments. The evaluation data is used by AT&T to immediately address and correct any deficiencies.

Student feedback is gathered after each training course through completion of automated online surveys. Surveys are presented at the end of training in which computers are used. For training where computers are not immediately available, students are given a handout with a link to the survey, and emails are sent to the students to remind them to complete the survey. We issue hard copy evaluation forms to those who do not have access to an online computer. Information from hard copy submissions is entered into a spreadsheet to facilitate analysis of data across courses. The aggregated evaluation data allows AT&T to identify areas for continuous improvement and correction of deficiencies with course content, instructors, facilities, format, method and/or delivery (including associated materials) related to any part of the EIS training program. In the event the CO or OCO provides written notice of unacceptable issues, AT&T uses these same procedures to thoroughly analyze the issue and make corrective action.

1.2 AT&T's Capability to Provide Customers with Web-Based Access to Support Systems [L.30.1(1)(b); M.2.2(2 of 3); G.5]

GSA and agencies will access our BSS through a fully compliant and user-friendly web portal. The details are provided in **Section 1.1.3** and throughout this proposal and select attachments.

2 Management Response to Requirements for Section E: Inspection and Acceptance [L.30(2); L.30.1(2); E]

Using industry standard best practices and our extensive commercial experience, AT&T has developed a rigorous approach and detailed processes for verification and testing of our systems and services in our commercial and government work.

2.1 AT&T Capability to Comply with the Requirements in Section E: Inspection and Acceptance [L.30.1(2)]

Introduction [E.1]: GSA and agencies need assurance that the systems and services used in support of the EIS contract meet service delivery needs. AT&T looks forward to fully cooperating with the GSA to execute testing as proof-points of AT&T's compliance. GSA has very high standards for BSS, security, and the services it provides to its customers through the EIS contract. GSA achieves those high standards by setting stringent requirements for the inspection and acceptance and security testing of the contractor provided BSS and EIS services.

We have refined our approach for government support through our support of GSA on the Networx and Crossover contracts. This experience gives AT&T a solid foundation of people, processes, technology and support systems ready to develop, test, verify and implement our BSS and EIS services. We are continuously improving our system capabilities and will provide the same rigor with the EIS BSS and EIS Services verification testing. **Table 2.1-1** highlights how AT&T strengths result in government benefits from AT&T's inspection and acceptance process.

Table 2.1-1. AT&T's EIS Service and BSS Testing. By setting high standards for testing and verification, GSA gains confidence in the quality, capability and security of AT&T's BSS and EIS services.

Evaluation Factor	Approach	Benefit	Capability
Quality of Systems	- Built on lessons learned from AT&T Networx BSS and commercial capabilities - Enhanced to address EIS technology refresh	- Confidence in dealing with proven systems, higher network performance and experienced personnel - Application of industry best practices throughout development and testing processes resulting in less down time and fewer failures	For Networx, AT&T performed testing on more than 10 projects per year where requirements modification required testing and validation – all completed on time and to customer satisfaction
Customer Access	Two-factor authenticated sign on through our commercial Business Center portal leads to EIS-specific Government Center portal	- Enhanced security that is continuously updated and improved - Ease of access to all BSS functionality - Facilitates government participation and observance of testing	

Evaluation Factor	Approach	Benefit	Capability
Ability	- Testing conducted by dedicated User Acceptance Testing (UAT) team - Testing team includes AT&T and government Subject Matter Specialists	- Reduces learning curve and brings best practices for faster and higher quality testing - Confidence that EIS-specific needs are fully addressed	

2.1.1 FAR 52.252 Clauses Incorporated by Reference (Feb 1998) [E.1.1]

AT&T acknowledges the FAR clauses in RFP Section E.1.1.1 as being included by reference at the contract and TO levels as applicable.

2.2 Test Methodology [E.2]

Management Approach, Techniques, and Tools

AT&T's approach to Inspection and Acceptance and BSS Testing follows a consistent methodology used for both government and commercial customers. To prepare for the BSS testing with GSA Conexus and to quickly execute the 13 BSS test cases, AT&T will first perform rigorous internal unit testing.

AT&T has tailored its standard approach to strictly comply with all requirements established in RFP Section E.2. Additional details of our approach are provided in **Sections 2.2.1** and **2.2.2**. Full details of our testing plans are provided at **Appendix C** and **Appendix D** to this volume.

UAT is a process to obtain confirmation by a subject matter specialist, preferably the owner or client of the object under test, through trial or review, that the system modification or addition meets requirements. When projects are initiated, we will compile a series of documents that contain detailed information related to the projects. Reviews with the client help to understand all requirements. Once requirements are approved, we will begin to develop a comprehensive end-to-end test package. This test package will be reviewed with the client/sponsor, project manager and other stakeholders and updated as needed. For EIS, the test package confirms the draft test plans included in this proposal and any changes incorporated by the government through the post-award approval processes. Once the test package is approved and our internal sign-offs are received, we will begin formal testing in dedicated test

environments utilization the actual code that will be deployed into final system production.

Each test case is tested to confirm that the code conforms to the business requirements. Using the Agile methodology, the code is continuously tested and retested before production deployment. All defects found during testing are documented from opening to closing in a separate system and are retested once fixed to confirm code is defect free before launch. Daily testing check points are conducted during the testing period. If additional defects are found after launch, we fix them in the production environment and record as production defects. These are also retested before production deployment. When testing is complete, a User Certification Test (UCT) or Regression Test will be conducted to verify that the code is correctly transferred and deployed to production. Security testing is built into all areas of testing from UAT through UCT, including regression test. If issues are discovered, they will be fixed and retested immediately. For EIS, AT&T notifies the government of test completion and gains final approval through the processes described in RFP Section E and as summarized in the paragraphs below and detailed in **Appendices C and D**.

2.2.1 Business Support Systems Verification Testing [E.2.1]

AT&T provides our draft BSS Verification Test Plan (BSS Test Plan) as **Appendix C** to this volume. Our final BSS Test Plan will be provided 30 days after NTP. If the government rejects our plan within 21 days of receipt, AT&T will update our plan based on government comments within 14 days of our receipt of government comments.

Figure 2.2.1-1 illustrates AT&T's Verification Test processes tailored specifically to the requirements for BSS Verification Testing.

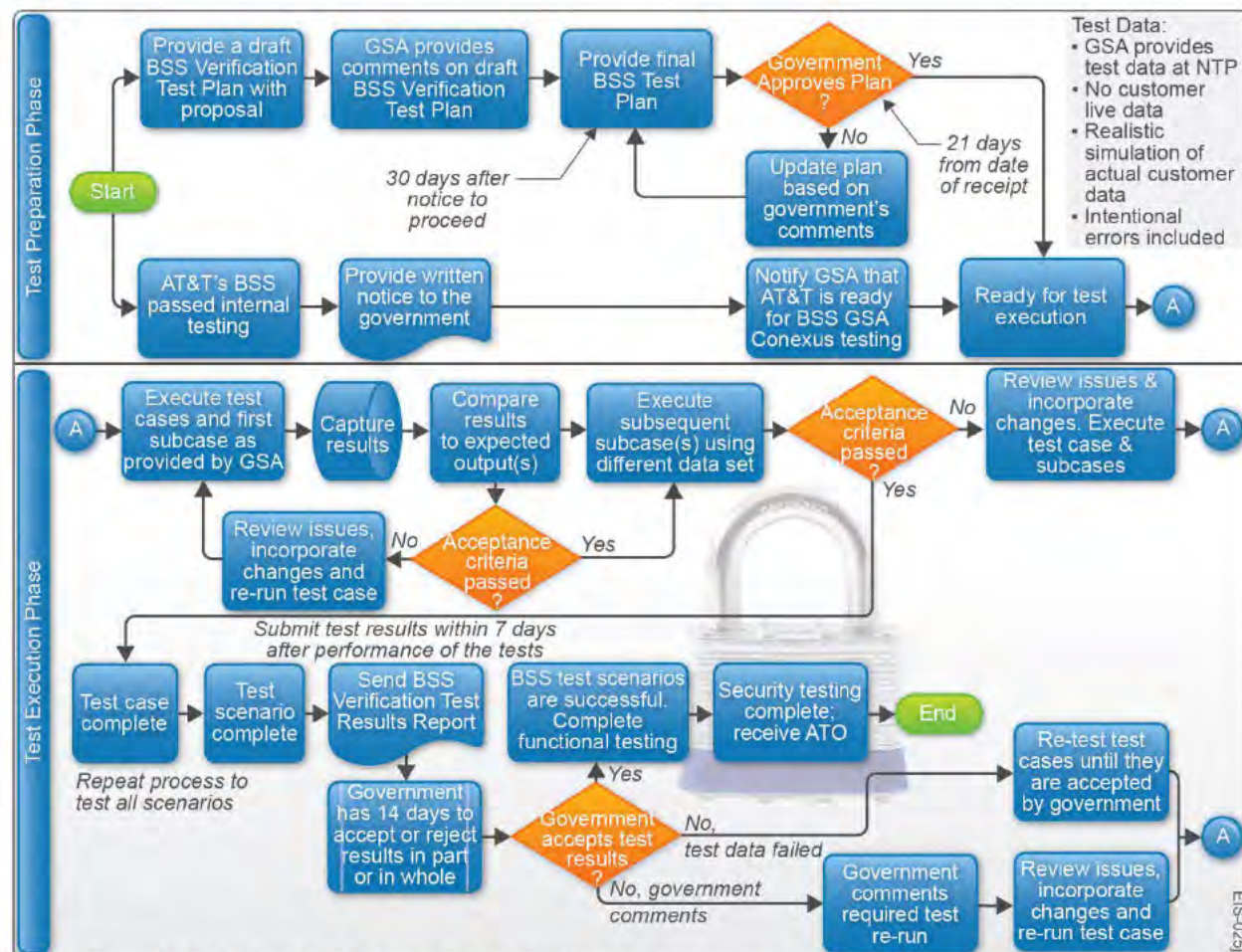


Figure 2.2.1-1. Testing Process Flow. GSA has specific requirements for verification and testing before acceptance. AT&T's Verification Testing Process Flow provides structure for the preparation and conduct of BSS verification testing and establishes confidence in our results.

AT&T accepts any opportunity offered by the government for preliminary testing before award but after submission of proposals. AT&T understands that such testing does not replace post-award formal testing, complies with all required primary security features such as anti-virus software, and accepts any terms and conditions issued by the government for the testing. If additional government comments are received, AT&T will again update its plan within 14 days and will repeat the update process until final approval is achieved. If awarded, AT&T will be eager to begin and complete BSS Testing to achieve BSS Final Contract acceptance well within 12 months of acceptance of our test plan in accordance with RFP Section G.2.3.

2.2.1.1 Scope [E.2.1.1]

AT&T will conduct BSS testing to meet all Inspection and Acceptance requirements described in RFP Section E.2.1.1. **Table 2.2.1-1** provides a crosswalk to the **Appendix C** reference where each of the requirements is covered in detail.

Table 2.2.1-1. BSS Inspection and Acceptance. *GSA is welcomed and encouraged to attend and observe the conduct of our comprehensive Verification, Inspection and Acceptance of our EIS BSS at our Oakton, Virginia facility.*

Inspection and Acceptance Requirements (E.2.1.1)	Appendix C Reference
▪ BSS Testing Verification That All BSS Functional, Regression, Load, and Security Requirements Have Been Successfully Met [L.30.2.3(1); E.2.1]	C-1.1
▪ Performance of BSS Testing for All Management and Operation Functions [L.30.2.3(2); E.2.1.1]	C-1.2
– Ordering [L.30.2.3(2); E.2.1.1]	C-1.2.1
– Billing [L.30.2.3(2); E.2.1.1]	C-1.2.2
– Inventory Management [L.30.2.3(2); E.2.1.1]	C-1.2.3
– Disputes [L.30.2.3(2); E.2.1.1]	C-1.2.4
– SLA Management [L.30.2.3(2); E.2.1.1]	C-1.2.5
– Trouble Ticketing [L.30.2.3(2); E.2.1.1]	C-1.2.6
▪ Security Testing Based on BSS Security Requirements [L.30.2.3(3); E.2.1.1]	C-1.3
▪ BSS Testing's Inclusion of Multiple Test Cases [L.30.2.3(4); E.2.1.1]	C-1.4
▪ BSS Testing's Inclusion of Use Cases for Quality, Utility, and Customer Access Features [L.30.2.3(5); E.2.1.1]	C-1.5
▪ Observance of BSS Verification Testing by Government Representatives [E.2.1.1]	C-1.6
▪ Performance of BSS Verification Testing [E.2.1.1]	C-1.7

2.2.1.2 BSS Test Scenarios [E.2.1.2]

2.2.1.2.1 Testing Prerequisites [E.2.1.2.1]

Before initiating formal BSS testing, AT&T will provide written notice to the government that our BSS has passed our internal testing and is ready to begin BSS interface with GSA Conexus. AT&T will also provide a final test plan that has been accepted by GSA. Verification and acceptance testing confirms that our BSS meets requirements in RFP Sections G and J.2. AT&T will support BSS security and functional testing as defined in RFP Sections G.5.6 and G.5.5.1. Additional details are at **Appendix C, Section C-2**.

2.2.1.2.2 Test Scenarios [E.2.1.2.2]

AT&T addresses test scenarios at **Appendix C, Sections C-3.1 – C-3.13** and **Table 2.2.1-2**. All test scenarios address the functional requirements defined in relevant portions of RFP Sections G and/or J.2, as shown for each scenario in the table at RFP Section E.2.1.2.2, and all associated test cases as shown in RFP Section E.2.1.3 and the subsections shown for each of the test cases. All scenarios address relevant data exchange mechanisms and validation of data exchanged. For each scenario, AT&T's

BSS must pass the test cases adhering to the defined acceptance criteria for both the test scenario itself and the associated test cases.

AT&T will accept and incorporate GSA's changes into our BSS test plan and execute the test cases [E.2.1.3] associated with each of the test scenarios [E.2.1.2] as shown in **Table 2.2.1-2**. Details of our test plan are found at **Appendix C** and specific paragraphs referenced in the table. AT&T's BSS must pass the test cases adhering to the defined acceptance criteria.

Table 2.2.1-2. Scenarios. *AT&T's comprehensive BSS Test Plan uses two or more data sets to conduct one or more tests against each of the 13 scenarios specified in RFP Section E.2.1.2.2.*

Section E Paragraph	Section E Requirement	Appendix C Reference
E.2.1.3.1	BSS-TS01: Direct Data Exchange	C-3; C-3.1
E.2.1.3.2	BSS-TS02: TO Data Management	C-3; C-2
E.2.1.3.3	BSS-TS03: Role-Based Access Control	C-3; C-3.3
E.2.1.3.4	BSS-TS04: Service Ordering	C-3; C-3.4
E.2.1.3.5	BSS-TS05: Supplements to In-Progress Orders	C-3; C-3.5
E.2.1.3.6	BSS-TS06: Administrative Change Orders	C-3; C-3.6
E.2.1.3.7	BSS-TS07: Rapid Provisioning & Self-Provisioning Orders	C-3; C-3.7
E.2.1.3.8	BSS-TS08: Inventory and Billing	C-3; C-3.8
E.2.1.3.9	BSS-TS09: Dispute Handling	C-3; C-3.9
E.2.1.3.10	BSS-TS10: SLA Management	C-3; C-3.10
E.2.1.3.11	BSS-TS11: Open-Format Reporting	C-3; C-3.11
E.2.1.3.12	BSS-TS12: Regression Testing	C-3; C-3.12
E.2.1.3.13	BSS-TS13: Security Testing	C-3; C-3.13

2.2.1.3 BSS Test Cases [E.2.1.3]

AT&T will incorporate changes into our BSS Test Plan and executes the test cases associated with each of the test scenarios as shown in the tables at RFP Section E.2.1.3. **Appendix C, Section C-3** and its subsections, provide additional detail about the test environment, and its terms and conditions that apply to AT&T's BSS testing.

Table 2.2.1-3 describes the test conditions, environment and standards of AT&T's BSS testing process.

Table 2.2.1-3. Test Environment and Conditions. *By adhering to the high standards of test Conditions, acceptance and environment established by GSA, AT&T gives GSA confidence in its test execution.*

Test Conditions, Data Content, and Acceptance	
AT&T accepts the following test conditions	- No testing between AT&T and GSA occurs until both the AT&T BSS and GSA Conexus have passed unit testing - All testing will be performed on the actual system to be used in delivering service (i.e., special purpose test systems are not used) - Unless otherwise specified, all data transfers are to use the mechanism specified in RFP Section J.2 for that data set.
AT&T will use GSA provided test data for all BSS verification	We understand and accept that this data will be used for testing purposes only; that no customer "live" data will be used for testing; that this data will be a realistic simulation of actual customer data; and that the test data

Test Conditions, Data Content, and Acceptance	
testing unless specified otherwise	includes, in some tests, intentional errors intended to test AT&T's BSS error handling.
AT&T's BSS testing follows a tiered approach	- AT&T accepts multiple test cases for the test scenarios defined in RFP Section E.2.1.2 - AT&T accepts and incorporates changes into the BSS Test Plan, and executes each test case with one or more test data sets - In providing test data sets, GSA will group them into Test Subcases: - Each Test Subcase contains data sets intended to test a specific real world test case (e.g., a complete and accurate disconnect order) - Each test subcase includes at least two complete test data sets.
BSS functional testing acceptance	- AT&T's BSS will not have completed functional testing until all BSS Test Scenarios (RFP Section E.2.1.2) are passed - A test scenario will not be considered passed until AT&T's BSS properly handles each associated test case - A test case is not considered passed until AT&T's BSS properly handles each associated subcase twice in succession using different data sets - A subcase is not considered passed until AT&T's BSS properly handles the data sets following the prescribed actions with no errors or warnings.
As described in detail at Appendix C, Sections C-3.1 - C-3.13, AT&T accepts, incorporates into our BSS test plan, and Successfully executes each test scenario and each test case defined at RFP Section E.2.1.3.	AT&T uses the definitions provided at RFP Section E.2.1.3, and our BSS must pass the test cases adhering to the defined acceptance criteria for each test scenario and all of the test cases associated with the scenario.

AT&T conducts BSS security testing acceptance in accordance within RFP Section G.5.6 and associated references.

2.2.1.4 Test Results [E.2.1.4]

AT&T's test results will demonstrate that it successfully meets the BSS acceptance criteria for the various test scenarios/test cases defined in RFP Sections E.2.1.2 and E.2.1.3. **Appendix C, Section C-5.2** describes how AT&T provides test results with details of testing.

2.2.1.5 Deliverables [E.2.1.5-E.2.1.5.2]

The Draft Verification Test Plan – is discussed in **Appendix C, Section C-5.1**.

The Draft Verification Test Results Report – is discussed in **Appendix C, Section C-5.2**.

2.2.2 EIS Services Verification Testing [E.2.2]

Appendix D contains EIS Services Test Plans, for each of the services offered by AT&T, as required. Our test methodology follows that described in RFP Section E.2.2: test scenarios, test cases, test data sets, acceptance criteria, and deliverables.

Figure 2.2.2-1 gives an overview of our verification testing process.



Figure 2.2.2-1. Verification Testing and Service Order Process. *Verification occurs during the service order process. The service-specific verification test plan is finalized after Service Order Confirmation and implemented before Service Order Confirmation Notification.*

2.2.2.1 General Testing Requirements [E.2.2.1]

AT&T's verification and testing approach for EIS services is at **Appendix D, Sections D-1 to D-12**, with associated subsections for each service offered. Our EIS Test Plan at **Appendix D** includes:

- Test methodologies for each service with test cases that define the parameters to be measured, the measurement procedure and the acceptance (pass/fail) criteria
- Fallback approach that describes our fallback process and procedures in case of testing failures. For each service verification test, if a test fails, appropriate and service-specific remediation will take place, followed by re-testing.
- Confirmation that AT&T provides a test plan for all new services offered during the life of the contract.

AT&T accepts the following conditions:

- Agencies may define additional testing in TOs
- AT&T allows and welcomes government representatives to observe all or any part of our EIS services verification testing
- AT&T provides all necessary test equipment, such as data terminals, load boxes, test cables, and any other hardware and software required for testing.

2.2.2.2 Test Scenarios [E.2.2.2; E.2.2.2.1]

Test Scenarios are provided by the government in RFP Section E.2.2.2. These three scenarios cover minimum service test scenarios for EIS. AT&T incorporates these scenarios into our plan on a service-specific basis as presented in **Appendix D**. AT&T is explicit on meeting FedRAMP and NIST security requirements for all bid services as required in RFP Section C.2.

2.2.2.3 Test Cases [E.2.2.3]

Test Cases are developed by AT&T for each service verification test. The details of these test cases are contained in the service specific test plan tables described in **Appendix D, Sections D-1 to D-12.**

2.2.2.4 Test Data Sets [E.2.2.4]

Test Data sets are developed by AT&T for each test case and service verification test. The details of these test data sets are contained in the service specific test plan tables described in **Appendix D, Sections D-1 to D-12.**

2.2.2.5 Test Results and Acceptance [E.2.2.5]

When service-specific verification testing is completed and the test results demonstrate compliance with acceptance criteria defined in our government accepted EIS Test Plan, AT&T will provide the government with a service-specific verification test report. AT&T will signal the completion of service-specific verification testing by issuing a SOCN for the service order that initiated the verification test. The verification test report will be specific to the service order that initiated the verification test process.

2.2.2.6 Deliverables [E.2.2.6]

AT&T provides its EIS Test Plan as **Appendix D** to this volume. Our EIS Test plan is based on the methodology described in RFP Sections E.2.2.1 – E.2.2.5. AT&T will update its Plan for all new services that are added to our contract with our modification proposal. AT&T will provide its EIS Testing Report as defined in RFP Section E.2.2.5 within 3 days of service installation and testing.

3 Management Response to Requirements for Section J.2: Contractor Data Interaction Plan [L.30(3); L.30.1(3); M.2.2(3 of 3); J.2]

AT&T will offer GSA and customer agencies a well-designed data interaction plan that provides specific and effective program of data exchange, collection, tracking, analysis, and reporting — all necessary to support the administration of the EIS contract.

3.1 AT&T's Capability to Comply with Section J.2: Contractor Data Interaction Plan [L.30.1(3)]

Introduction [J.2.1]: GSA continues to make its own technological innovations such as the development and fielding of its new Conexus system for exchanging information with its contractors and supported agencies. Thus, GSA needs its contractors with the

depth and breadth of capabilities to work within existing GSA Systems and simultaneously be prepared to rapidly adapt to new technologies and systems. AT&T builds upon the systems and experienced personnel that have supported GSA and its agency customers on the Networx and regional contracts to achieve effective and fully compliant data interaction capabilities for EIS. At the same time, AT&T's commercial business and our strong investment in innovation make us ideally suited to work with GSA's developing data exchange environment. This enables low risk performance and a seamless transition. **Table 3.1-1** provides detail on our data interaction approach, its benefits and our supporting capabilities.

Table 3.1-1. Secure, Efficient CDIP-Compliant Data Exchange. *EIS customers receive large agency-tested responsive delivery of web services with "hardened" security controls for reliable data exchange.*

AT&T Features	GSA and Agency Benefits
- SOAP based web services over HTTPS for transactions and Secure Shell (SSH) File Transfer Protocol allow for large volumes data transfers - As a GSA Networx prime contractor, AT&T has extensive experience with similar deliverables and underlying government/contractor datasets required for all the EIS management and operation functions.	- Secure, automated mechanisms for direct transfer of transaction data to the government's systems - No learning curve allows faster and more reliable communications between government and AT&T systems
- AT&T's Business Center portal provides Role-Based Access Control (RBAC) to allow only authorized users with appropriate permissions access to BSS - Transmission of inventory snapshot and invoice data to GSA and agencies build on capabilities existing on the Networx contract.	- Flexibility for customer to access their data at their convenience through AT&T's Business Center - Effortless agency setup of data exchange for inventory, invoice, and other deliverables.
Extensive eBonding experience with government and commercial customers enables smooth implementation of system-to-system interaction with GSA's next-generation network solutions management system.	Highly secure automated transmission of invoice data. Clearly defined SFTP or Web Services for each deliverable.

AT&T clearly defines SFTP or Web Services for each deliverable by providing the government our AT&T-defined data formats to support government-defined application programming interfaces that meet or exceed EIS data interaction requirements.

3.1.1 EIS Management and Operations: High-Level Process Diagram [J.2.1.1]

Figure 3.1-1 depicts our BSS high-level process flow and data exchange mechanisms with GSA Systems/GSA Conexus for the ordering, billing, disputes, inventory management, and SLA management life cycle functions.



Figure 3.1-1. CDIP High-Level Process Flow. *Agency-approved transfer mechanisms support highly secure exchange of data between GSA Systems/GSA Conexus and AT&T's BSS.*

The AT&T Business Center BSS Platform supports CDIP Acquisition/Task Order process flows, transfer mechanisms, data exchanges, and common operational requirements including:

- Supporting initial TO setup, including changes caused by TO modifications, new information from the customer, and BSS changes approved by GSA
- Supporting all TO data management process steps defined in RFP Section J.2.3.2
- Supporting all TO related deliverables and data exchange defined in RFP Section J.2.3.3
- Accepting/Collecting Direct Billed Agency Setup (DBAS) data set from the government customer

3.2 Common Data Interaction Requirements [J.2.2]

Baseline operating procedures are necessary to make sure that all engaged parties understand controls and guidelines; otherwise, uncontrolled changes could cause errors in the data, which would lead to errors or gaps in management of the contract. Based upon the requirements stated in RFP Section J.2.2 and summarized in **Table 3.2-1**.

AT&T understands and accepts that requests for exceptions to the CDIP submission requirements must be authorized by the GSA or customer CO, depending upon the type of exception requested for consideration, and that incorrect deliverables must be resubmitted quickly, within three days of determination. Throughout the operation of the Networx contracts, AT&T has developed cooperative operating relationships with both the GSA and our customer agencies, which has led to well-controlled change executions. AT&T looks forward to continuing on the EIS contract.

Table 3.2-1. Common Data Interaction Requirements. GSA uses common requirements to manage change and maintain control of the data environment.

EIS CDI Requirement	Common Data Interaction (CDI) Requirements [J.2.2]
Relevant Contracting Officer [J.2.2.1]	Where exceptions are allowable within the CDIP, AT&T understands and accepts that any exceptions to CDIP data submission requirements must be authorized, in writing, by the relevant CO — the GSA CO for GSA, or the OCO for customers.
Resubmission of Incorrect Deliverables [J.2.2.2]	If AT&T becomes aware of an error in a previously submitted deliverable, regardless of how the error was discovered, AT&T resubmits the deliverable within three (3) days of becoming aware of the error with the exception of billing errors identified after the government makes payment, which requires the submission of a billing adjustment as described in RFP Section J.2.5. AT&T also notifies the relevant COR and CO via email of the error and the action taken.
Deliverable format, Content, and Transfer Mechanism [J.2.2.3]	While TO specifications do not override GSA deliverable requirements, AT&T will provide alternative formats, contents, and transfer mechanisms for deliverables only when an exception is authorized by the GSA CO for GSA deliverables and the OCO for customer deliverables.
Scope of Deliverables [J.2.2.4]	AT&T verifies that the scope of deliverables is at the TO level, unless otherwise specified within the contract. AT&T understands that any exceptions must be authorized by the GSA CO or customer's OCO.

3.3 Task Order Data Management [J.2.3]

Upon award of each Task Order under EIS, GSA and AT&T must update data infrastructures to incorporate specific data elements defined within the Task Order and necessary to administration of the contract. These elements will be kept current throughout the life cycle of the TO. AT&T's data management processes and exchanges provide for the initial setup, ongoing maintenance and update of task order data in GSA's Systems and our BSS. This includes exchange between GSA Systems/GSA Conexus and AT&T's BSS of Task Order Controlled Data, Task Order Associated Data, and System Reference Data as shown in **Figure 3.3-1**.



Figure 3.3-1. CDIP-Task Order. Data Management Process Flow. Automated and highly secure transfer of Task Order data is fully compliant with EIS requirements and cover the three categories of data exchanged

3.3.1 Common Operational Requirements [J.2.3.1]

AT&T will adhere to the common operational requirements noted in RFP Section J.2.3.1. AT&T will submit data via GSA Systems [J.2.3.1.1]. In order to allow only authorized users with appropriate permissions access to BSS, AT&T provides highly secure RBAC [J.2.3.1.2] via the Business Center.

- AT&T captures and stores a list of users and user permissions that include authorized users for restricted access and restricts access accordingly
- AT&T adds new users within seven days of customer request
- AT&T removes users who are no longer authorized within one business day of notification or sooner if needed.

3.3.2 Task Order Data Management Process [J.2.3.2]

GSA requires a strict process by which GSA and AT&T systems are prepared to process service orders. This process will make sure that both government and provider systems are able to effectively exchange and process data once transactions begin passing between systems. After successful completion of BSS verification and security testing, GSA will provide AT&T with System Reference Data [J.2.3.2.1]. AT&T will follow the process that GSA has prescribed, as illustrated in



Figure 3.3-2. Task Order Data Management Process. Initial system reference and TO data is setup between GSA and AT&T systems before processing TO service orders.

Figure 3.3-2.

AT&T will configure the BSS to submit data based upon the provided system reference data. This must be complete before processing any TO on the contract.

TO Data [J.2.3.2.2]: Upon TO award, AT&T will follow the process provided by GSA and will provide all required TO setup data points and follow all process steps at the initial setup of each TO, including the Direct-Billed Agency Setup (DBAS) data to GSA. Service orders within the Task Order will not be provisioned or provided until this initial setup activity is complete. GSA will provide updates to the system reference data sets on an as needed basis. A contract modification will not be issued for such updates.

3.3.3 Deliverables and Data Exchange [J.2.3.3]

In support of the setup processes, GSA and AT&T will exchange a list of predefined data sets. **Table 3.3-1** depicts the categories and ownership of these data sets.

Table 3.3-1. Deliverables and Data Exchange. *Data management interchange is 100% compliant.*

Deliverables and Data Exchange [J-2.3.3]	
Government-Provided Data: System Reference [J.2.3.3.1]	AT&T receives the reference data sets listed in the table at RFP Section J.2.3.3.1 with detailed contents as specified in RFP Section J.2.10.2. For each of these data sets, AT&T supports all data transfer mechanisms as defined in RFP Section J.2.9 and depicted in Figure 3.3-1 and Figure 3.3-2 above.
AT&T-Provided Data Sets: Deliverables [J.2.3.3.3]	AT&T provides deliverable as listed in the table at RFP Section J.2.3.3.3 with detailed contents as specified in RFP Section J.2.10.2. For each of these data sets, AT&T supports all data transfer mechanisms as defined in RFP Section J.2.9.

3.4 Ordering [J.2.4]

Following initial contract and Task Order data setup, AT&T is ready to process orders. Orders can either be defined in the TO or defined separately after the TO. **Figure 3.4-1** depicts an overview of our CDIP process for ordering data.

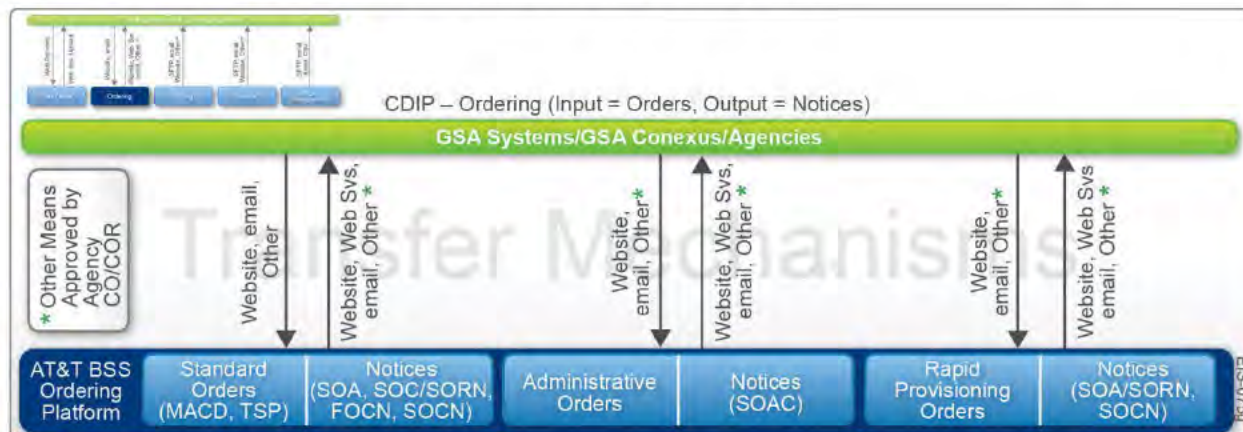


Figure 3.4-1. Order Data Interchange Flow. GSA and agencies benefit from AT&T's well-designed and fully compliant data interchange for Ordering.

3.4.1 Common Operational Requirements [J.2.4.1]

Across orders, there are some common operational requirements with which AT&T complies. **Table 3.4-1** lists the ordering requirements AT&T addresses with our CDIP.

Table 3.4-1. CDIP Common Operational Requirements. *Common Operational Requirements provide structure across multiple ordering types.*

Common Operational Requirements [J.2.4.1]	
Task Orders [J.2.4.1.1]	Whether orders are included with the TO or are submitted subsequently, AT&T will follow the requirements and processes described within RFP
Data Field	Compliance

Common Operational Requirements [J.2.4.1]	
Agency Hierarchy Code [J.2.4.1.2]	- AT&T tracks AHCs on all services provided from order submission through disconnection - AT&T validates the presence of an AHC on all orders - AT&T supports AHC changes to a provisioned order without interruption of service.
Unique Billing Identifier [J.2.4.1.3]	- UBIs link together items for ordering, billing, and inventory management - AT&T creates UBIs as described in RFP Section J.2.10.1.1.2 - AT&T provides the UBI as a data element in the SOCN.
Agency Service Request Number [J.2.4.1.4]	- If provided by the government, AT&T will include the ASRN as a data element(s) on all deliverables that reference the order or the services included in the order tracks all ASRNs from order submission through disconnection - If the government provides ASRN data element(s) as part of a Service Order (SO), AT&T will include them on all deliverables that reference that order or the services included in that order.
Contract Line Item Number [J.2.4.1.5]	- AT&T will provide CLIN and associated ICB data elements for each line item in all ordering deliverables per RFP Section J.2.3.3.3 - AT&T matches CLINs reported on billing files to those on the SOCN for that particular order.
Common Elements	
Ordering Data Sets and Notifications [J.2.4.1.6]	AT&T exchanges data sets with the government, via order notifications, as listed in RFP Section J.2.4.1.6 as part of the ordering process. A TO can override deliverable timing so long as notices remain in the order specified in RFP Section J.2.4.2 and all notices are provided before billing. The standard data sets are: - Service Order (SO) - Service Order Acknowledgement (SOA) - Service Order Confirmation (SOC) - Service Order Rejection Notice (SORN) - FOCN - SOCN - Service Order Administrative Change (SOAC) - SSCN.
Auto-Sold CLINs [J.2.4.1.7]	- AT&T includes any auto-sold CLINs in all notices and deliverables that require reporting CLINs - Unless otherwise specified in the SO or TO, applies the AHC listed for the base CLIN to all associated auto-sold CLINs - Unless otherwise specified in the SO or TO, applies the ASRN(s) listed for the base CLIN to all associated auto-sold CLINs - AT&T manages activation and deactivation of auto-sold CLINs in accordance with RFP Section J.2.4.1.10 and RFP Section J.2.4.2.5.
Order Types [J.2.4.1.8]	AT&T will expect each order submitted by the customer to have an overall order type and each line item to have a line item order type.
Splitting Complex Orders into Suborders [J.2.4.1.9]	In the event that AT&T needs to split orders into logical suborders the following restrictions will be applied: - Services logically linked by a Service Grouping ID as described in RFP Section J.2.10.1.1.2 are not split across multiple suborders - AT&T does not split any SO into suborders if the SO or the TO contains instructions prohibiting such splitting.
Service State [J.2.4.1.10]	AT&T acknowledges and adopts the definitions of service states applicable to each provisioned service, as defined by a single UBI. AT&T supports the following government service state requirements: - AT&T validates that all provisioned UBIs have a valid service state assigned at all times: - A UBI is not considered provisioned before the SOCN for its installation - A UBI is not considered provisioned after the SOCN for its disconnection AT&T will not change the service state of a UBI except in response to direct government action (or as required based on predefined criteria captured in the contract or the TO).

3.4.2 Ordering Process [J.2.4.2]

So that GSA Systems have the most current view of order and inventory activity, AT&T will provide numerous order-related deliverables to GSA. If requested, such deliverables will also be provided to the customer.

Standard Orders [J.2.4.2.1] including moves, adds, changes (excluding ACO), and disconnects follow the process outlined in RFP Section J.2.4.2. **Figure 3.4-2** shows a typical order flow. In addition:

- If a SORN is issued, it will apply to the entire order, not individual line items
- If AT&T needs to split a complex SO into suborders, the standard order process will apply to each suborder
- If the government reports a problem within the acceptance period following order completion, AT&T will resolve and submit a new SOCN.

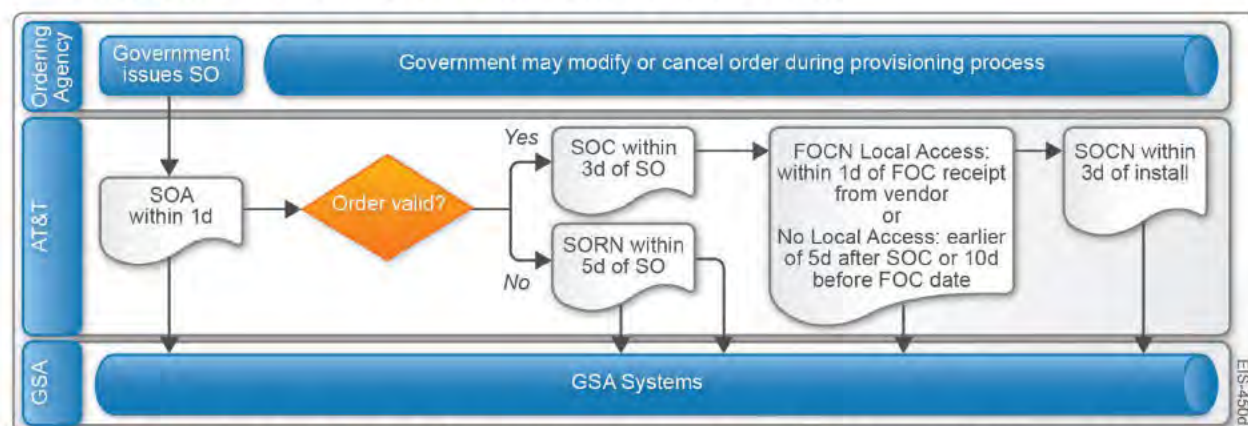


Figure 3.4-2. Typical Order Flow. AT&T's response to orders follows GSA's prescribed processes and timelines.

Table 3.4-2 below details the various other order types and associated deliverables.

Table 3.4-2. Order Types and Responses. Various types of orders trigger responses to GSA by AT&T.

Deliverable	Compliance
Telecommunications Service Priority (TSP) Orders [J.2.4.2.2]	If the government submits a Telecommunications Service Priority (TSP) order the standard process (see RFP Section G.3.3.3.1) applies with the following caveats: ▪ AT&T will follow the prioritizations applicable to TSP orders ▪ AT&T will not delay the delivery of services in any way based on the need to submit deliverables specified in this process.
Administrative Change Orders [J.2.4.2.3] Administrative Change Restrictions [J.2.4.2.3.1] Administrative Change Order Process [J.2.4.2.3.2]	▪ ACO may only modify government-provided inventory data points that have no impact on service delivery or pricing. Data elements beyond ASRN 1, ASRN 2, and AHC could also be addressed via ACO with mutual agreement between AT&T and GSA. ▪ Upon receipt of an ACO, AT&T will make the required updates and will submit a SOAC within seven days of the change order. The SOAC will be submitted to GSA, and, if requested, to the customer. Other order notices are not required.
Rapid Provisioning [J.2.4.2.4]	AT&T's rapid provisioned services include Ethernet Bandwidth on Demand and Cloud Services as defined by NIST, and as referenced in RFP Section C.2.5.

Deliverable	Compliance
Service State Changes [J.2.4.2.5]	If a service (defined by a single UBI) changes from one state to another (as defined in RFP Section J.2.4.1.10), AT&T will issue a SSCN within 24 hours. AT&T may combine multiple notices as individual line items on a single SSCN provided all notices are submitted within 24 hours of the individual state change.
Supplements or Updates to In-Progress Orders [J.2.4.2.6]	If it is necessary to supplement or update an in-progress order, the government will issue a supplement SO. AT&T's Service Request Number (CSRN) reported on the SOA will be the same as that reported on the original order: ▪ AT&T will submit an SOA in response to the supplement SO within one (1) business day ▪ If AT&T determines that the supplement SO is invalid, a SORN is submitted within three (3) days of the supplement SO. The CSRN reported on the SORN will be the same as that reported on the original order. ▪ AT&T will update the original order with the new data ▪ If any changes are required to data sets already submitted in response to the original order (e.g., SOC, FOCN), AT&T will issue updated versions of those notices. ▪ AT&T will complete the provisioning of the original order with updated information as described in the applicable order process.

3.4.3 Deliverables and Data Exchange [J.2.4.3]

In support of order deliverables, the government and AT&T will exchange a list of predefined data sets. As shown in **Table 3.4-3**, AT&T supports all required transfer mechanisms for each data set for ordering.

Table 3.4-3. Ordering Deliverables and Data Exchange. GSA receives data sets from AT&T but does not provide any to AT&T as part of the ordering process.

Deliverables and Data Exchange [J.2.4.3]	
Government-Provided Data Sets [J.2.4.3.1]	AT&T supports all required transfer mechanisms for each data listed in the table at RFP Section J.2.4.3.1 and as defined in RFP Section J.2.9.
Contractor-Provided Data Sets [J.2.4.3.2]	AT&T provides data set deliverables specified in the table at RFP Section J.2.4.3.2 at the frequency and via the transfer mechanisms shown in that table. We support all required transfer mechanisms for each data set as defined in RFP Section J.2.9.

3.5 Billing [J.2.5]

In order to accurately account for taxpayer dollars spent in support of necessary government activities, it is important for the government to receive an accurate and timely invoice. **Figure 3.5-1** depicts our CDIP process for billing data.

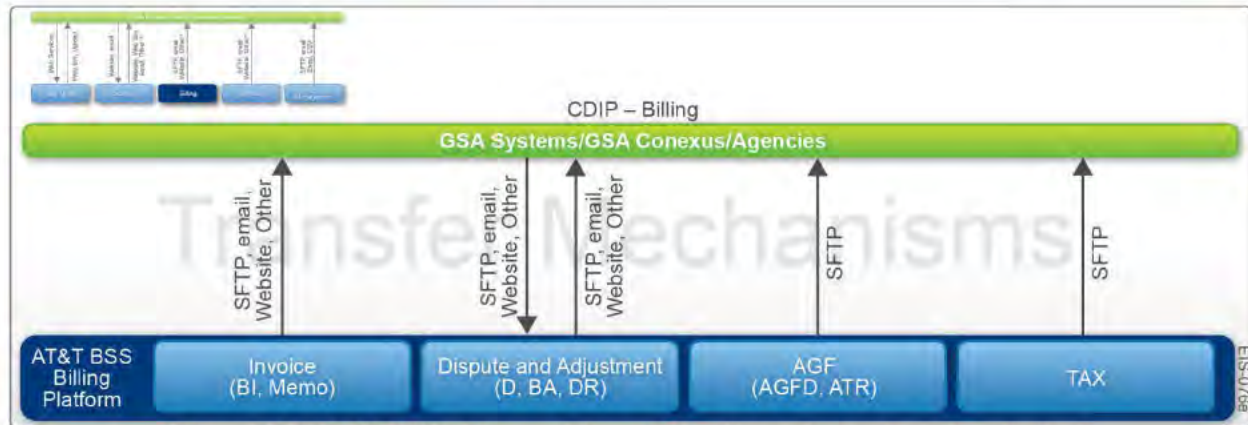


Figure 3.5-1. CDIP-Billing Process Flow. GSA and agencies receive automated and highly secure transfer of Billing-related data that is fully compliant with EIS requirements.

3.5.1 Common Operational Requirements [J.2.5.1]

AT&T's system design fully takes into account the need for an order to be accurately reflected on an invoice, and for GSA and agencies to receive useful billing data sets.

Table 3.5-1 provides details of our billing processes.

Table 3.5-1. CDIP Billing. AT&T fulfills 100% of the CDIP billing requirements.

Common Operational Requirements [J-2.5.1]	
Billing Cycle [J.2.5.1.1]	AT&T complies with the government's defined billing cycle, which runs from the first through the last day of the calendar month
Unique Billing Identifier [J.2.5.1.2]	AT&T systems design assures that the UBI reported on billing deliverables matches the UBI included on the SOCN for a particular element.
Contract Line Item Number [J.2.5.1.3]	- AT&T provides the CLIN and any associated ICB data element(s) for each line item in all billing deliverables - AT&T systems design confirms that the CLINs reported on billing deliverables match those included on the SOCN for a particular order.
Associated Government Fee [J.2.5.1.4]	- AT&T calculates the AGF as described in RFP Section J.2.10.1.1.1 - AT&T provides the AGF as a data element in billing deliverables - For TOs set up with direct billing, AT&T collects the AGF on behalf of GSA and transfers funds as described in RFP Section G.4.6.
Proration [J.2.5.1.5]	For services not delivered for the full calendar month billing cycle, AT&T applies the following proration requirements.
Proration formula [J.2.5.1.5.1] Service Change Order Proration [J.2.5.1.5.2]	AT&T will deploy Normalized 30-Day Month Proration, defined in Section J.2.5.1.5.1.2 to handle proration for services not delivered for the full calendar month billing cycle. AT&T will indicate the proration type of Normalized 30-Day Month Proration, defined in Section J.2.5.1.5.1.2, in the response to customer agency solicitations. Solicitation responses to unsupported proration type requests will clearly communicate AT&T does not currently support the requested proration type. AT&T may add support for a previously unsupported proration type at any time without contract modification by following the BSS Change Control process in Section G.5.5.1. AT&T will complete successful retesting of the BSS test cases associated with proration prior to billing. If Billable Days from Step 2 is equal to or greater than 30, proration does not apply; AT&T will bill the full MRC for that month. Service Change Order Proration process described in RFP Section J.2.5.1.5.2, treating the change as two connected events (previous service price end and new service price start) and calculating prorated billing amounts for each of the events.

Common Operational Requirements [J-2.5.1]	
Rounding [J.2.5.1.6] Rounding Requirements [J.2.5.1.6.1] Rounding Standards [J.2.5.1.6.2] Rounding Example Table [J.2.5.1.6.3]	- AT&T complies with the rounding requirements for storage of charges and use in all calculations to six decimal places for service price, prorating, taxes, fees, and surcharges when calculating summary data (including total cost) and when totaling the entire submitted bill - AT&T complies with standards for rounding to reach 6 decimal place values and rounding to reach 2 decimal place values - AT&T acknowledges and understands the rounding examples shown in RFP Section J.2.5.1.6.3 and will apply the rounding rules as described and as illustrated.
Taxes, Surcharges, and Fees [J.2.5.1.7]	AT&T complies with the following data requirements for taxes and surcharges: - Taxes are applied to each taxable line item as an aggregated total per billing line item - AT&T provides the detail composition of the aggregated tax on the Tax Detail (TAX) deliverable - AT&T does not aggregate taxes, surcharges, and fees into any other data element unless the TO specifies such aggregation (fully-loaded pricing) as described in RFP Sections H.14 and H.23.
Billing Level [J.2.5.1.8]	AT&T submits billing deliverables as described in Section J.2.5.2, using a TO billing level where each deliverable covers only a single TO unless the TO specifies another billing level where each deliverable covers only a single TO unless the TO specifies another billing level
Billing Data Sets [J.2.5.1.9]	AT&T will provide the required billing data sets exchanged between the government and AT&T as part of the ordering process. The standard data set deliverables are: - Billing Invoice (BI) - Billing Adjustment (BA) - Tax Detail (TAX) - AGF Detail (AGFD) - AGF Electronic Funds Transfer Report (ATR) - Monthly Billing Information Memorandum. AT&T will include on the BI all taxes, fees, and surcharges as described in Section J.2.5.1.7 and will not include any credits or adjustments.

3.5.2 Billing Process [J.2.5.2]

In support of accurate and timely billing, AT&T will apply this standard billing process to all TOs. All deliverables described below in **Table 3.5-2** will be provided to GSA no later than the 15th business day of the month and, if requested, will be provided to the customer. They will be based upon the billing levels defined in RFP Section J.2.5.1.8.

Table 3.5-2. Billing Process Deliverables. GSA receives timely and accurate billing deliverables from AT&T and prompt attention to any errors discovered.

Billing Process [J.2.5.2]	
Billing Deliverables	- Billing Invoice (BI) - Tax Detail (TAX) unless the TO specifies loaded pricing - Monthly Billing Information Memorandum (to customer only), if required to clarify any line items on the BI - Billing Adjustment (BA), if applicable.
Billing Deliverables to GSA Only	- AGFD - ATR

If the government determines that the BI is valid in its entirety, AT&T will receive payment in full. If the government determines that the BI is not valid, in whole or in part, it will initiate a billing dispute and enter the dispute process. The government may withhold payment to AT&T, in whole or in part, as specified in RFP Section G.4.4 and further clarified in RFP Section H.32. If required to correct errors identified after payment, AT&T will submit a BA, although this does not apply to errors that have resulted in disputes.

3.5.3 Deliverables and Data Exchange [J.2.5.3]

Table 3.5-3 describes deliverables and data exchange associated with the billing processes.

Table 3.5-3. Billing Process Deliverables and Data Exchange. GSA receives accurate and fully compliant deliverables from AT&T as part of the billing processes.

Deliverables and Data Exchange [J.2.5.3]	
Government-Provided Data Sets [J.2.5.3.1]	AT&T acknowledges that the government will not provide any data sets as part of this process.
AT&T-Provided Data Sets [J.2.5.3.2]	AT&T provides the following deliverables as part of the billing process. Detailed contents of each data set comply with RFP Section J.2.10.2. For each data set, AT&T supports all required transfer mechanisms as defined in RFP Section J.2.9: ▪ Billing Invoice (BI) ▪ Billing Adjustment (BA) ▪ Tax Detail (TAX) ▪ AGFD ▪ ATR ▪ Monthly Billing Information Memorandum

3.6 Disputes [J.2.6]

While systems and processes are designed to avoid errors, errors might still occur. Therefore, process and data exchange guidelines are necessary to facilitate timely resolution of any found errors. AT&T is fully compliant with the requirements for Billing and Inventory Disputes and the required data interchange and frequencies.

Figure 3.6-1 depicts our understanding of this data interchange flow and data transfer mechanisms.

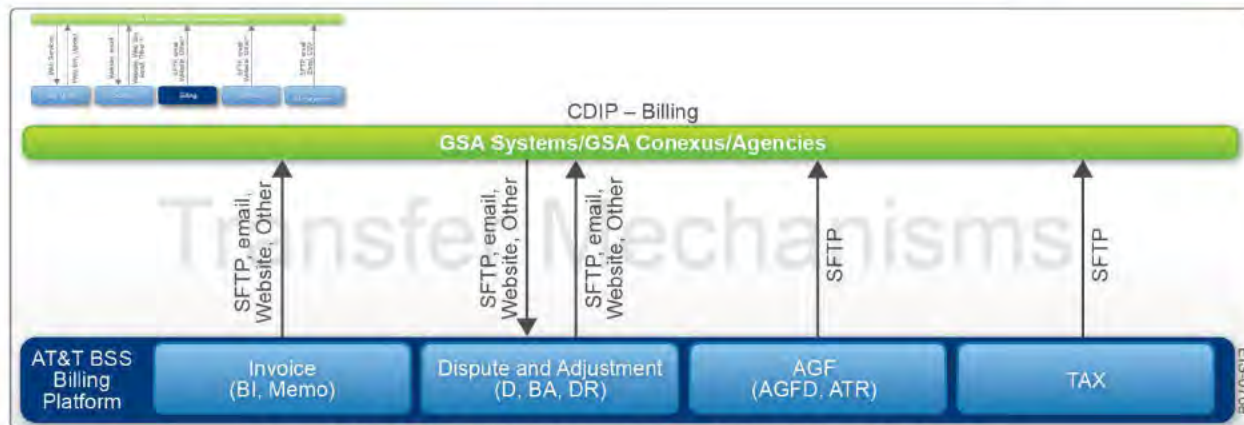


Figure 3.6-1. CDIP-Billing Process Flow. Automated and highly secure transfer of Billing-related data is fully compliant with EIS requirements.

Table 3.6-1 lists the billing and dispute requirements AT&T addresses with our CDIP.

Table 3.6-1. CDIP Disputes Requirements. AT&T fulfills 100% of the CDIP billing and disputes requirements.

CDIP Dispute Requirements	
Disputes [G.4.4; J.2.6]	
Common Operational Requirements [J.2.6.1]	AT&T understands and accepts the conditions under which the dispute process applies. The government disputes: - The content of a BI submitted by AT&T - The content of an Inventory Reconciliation (IR) submitted by AT&T - An SLACR Response submitted by AT&T.
Dispute Process [J.2.6.2]	AT&T will submit Dispute deliverables to both the customer and to GSA: - If the government is opening the dispute, it will submit a Dispute data set - AT&T works with the government to resolve the dispute - NLT the 15th business day each month, AT&T submits a DR - Upon resolution, AT&T applies any applicable credits within two (2) bill cycles.
Deliverables and Data Exchange [J.2.6.3]	
Government-Provided Data Sets [J.2.6.3.1]	The government will provide the Dispute as part of this process. AT&T supports all required transfer mechanisms as defined in RFP Section J.2.9.
AT&T-Provided Data Sets [J.2.6.3.2]	AT&T provides the Billing Adjustment (BA) and Dispute Report (DR) as part of this process. AT&T supports all required transfer mechanisms as defined in RFP Section J.2.9.

3.7 Inventory Management [J.2.7]

Inventory data is a product of order data exchange activities. As orders complete (i.e., SOCN), the inventory is updated to reflect the most current state of inventory elements. AT&T is fully compliant with Inventory Management and the required data interchange frequencies. **Figure 3.7-1** depicts our understanding of this data interchange flow.



Figure 3.7-1. CDIP-Inventory Process Flow. Automated and highly secure transfer of Inventory data is fully compliant with EIS requirements.

Table 3.7-1 lists the inventory requirements AT&T addresses with our CDIP.

Table 3.7-1. CDIP Inventory Requirements. Inventory process and structure assure GSA and agencies of accurate, complete inventories.

EIS CDIP Inventory Requirement	
Common Operational Requirements [J.2.7.1]	
GSA Conexus Inventory [J.2.7.1.1]	AT&T acknowledges that GSA will use data passed from AT&T to GSA's Conexus to support inventory validation.
Agency Hierarchy Code [J.2.7.1.2]	- AT&T supports AHC changes without an interruption of service - AT&T provides the AHC as a data element in the Inventory Reconciliation (IR) deliverable. - The AHC will be tracked for all services from order through disconnection
Unique Billing Identifier [J.2.7.1.3]	AT&T's system design assures that the UBI reported on the IR matches the UBI included on the SOCN and BI for a particular element
Inventory Management Process [J.2.7.2]	
Inventory Management Process [J.2.7.2]	Inventory management deliverables will be submitted to GSA and, if requested, to the customer. AT&T will follow the following inventory management process: - AT&T submits an IR deliverable monthly, NLT the 15th day of the month - If AT&T identifies a discrepancy in a previously submitted IR, we submit a corrected IR within 3 days of identifying the discrepancy. If the government identifies a discrepancy in the IR, it will follow the dispute process.
Deliverables & Data Exchange [J.2.7.3]	
Government-Provided Data Sets [J.2.7.3.1]	The government will not provide any data sets as part of this process.
AT&T-Provided Data Sets [J.2.7.3.2]	AT&T provides the Inventory Reconciliation (IR) as part of this process. AT&T supports all required transfer mechanisms as defined in RFP Section J.2.9.

3.8 SLA Management [J.2.8]

SLAs are a key component to effective contract management. AT&T's system design is fully compliant with requirements for SLA management including the required data interchange frequencies. **Figure 3.8-1** depicts our understanding of this data interchange flow and data transfer mechanisms.

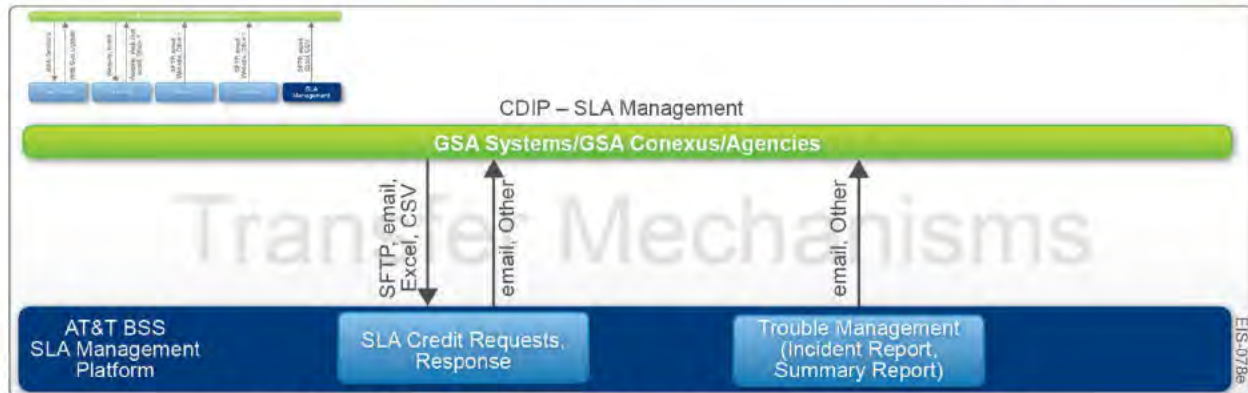


Figure 3.8-1. CDIP-SLA Management Process Flow. Automated and highly secure transfer of SLA Management data is fully compliant with EIS requirements.

Table 3.8-1 lists the SLA Management requirements AT&T addresses with our CDIP.

Table 3.8-1. CDIP SLA Management Requirements. SLA Management is facilitated by AT&T's fully compliant SLA Management processes.

SLA Management Requirements [G.8 J.2.8]	
Common Operational Requirements [J.2.8.1]	
SLA Measurement [J.2.8.1.1]	AT&T proactively measures each applicable SLA in accordance with its definition, capturing its performance relative to each KPI associated with the SLA as described in RFP Section G.8.3.1.
SLA Credit Requests [J.2.8.1]	In the event of a missed SLA, the government shall issue a credit request within six (6) months of the SLAR containing the SLA failure. AT&T reviews such requests and respond as indicated in RFP Section G.8.4.1.
SLA Management Process	
SLA Management Process [J. 2.8.2]	AT&T will submit deliverables associated with the SLA Management Process to GSA and, if requested, to the customer.
SLA Reporting Process [J.2.8.2.1]	- AT&T measures each KPI associated with each applicable SLA as described in RFP Section G.8 - AT&T submits a Service Level Agreement Report (SLAR), which captures its performance on all applicable SLAs and associated KPIs monthly, NLT the 15th day of the month - AT&T submits supplementary reports quarterly: - Trouble Management Performance Summary Report - Trouble Management Incident Performance Report.
SLA Credit Process [J.2.8.2.2]	- The government issues an SLA Credit Request (SLACR) within six (6) months of the SLAR containing the SLA failure - AT&T submits a SLACR response within 30 days of the SLACR - If AT&T accepts the government's finding, the credit is reflected on a BA within two (2) billing cycles of the SLACR response - If AT&T disagrees with the government's finding, the government may use the dispute process as defined in RFP Section G.4.4 and RFP Section J.2.6.
Deliverables and Data Exchange [J.2.8.3]	
Government-Provided Data Sets [J.2.8.3.1]	The government provides the SLA Credit Request (SLACR) as part of this process. AT&T supports all defined transfer mechanisms as defined in RFP Section J.2.9.
AT&T-Provided Data Sets [J.2.8.3.2]	AT&T provides the following deliverables. AT&T supports all required transfer mechanisms as defined in RFP Section J.2.9: - Service Level Agreement Report (SLAR) - SLACR Response - Trouble Management Performance Summary Report - Trouble Management Incident Performance Report - Billing Adjustment (BA).

3.9 Data Transfer Mechanisms [J.2.9]

In order to enable orderly data exchanges between the government and AT&T, we support all data transfer mechanisms required for each data set. **Table 3.9-1** provides details of AT&T compliance.

Table 3.9-1. Data Transfer Mechanisms. AT&T's BSS supports all mandatory and optional data transfer mechanisms associated with EIS.

Data Transfer Mechanisms	
Common Operational Requirements	
Common Operational Requirements [J.2.9.1]	▪ Governance of Exceptions: AT&T understands that exceptions to the data transfer mechanisms and associated requirements described below may only be authorized by the relevant CO. This will maintain the accuracy and effectiveness of the data exchanges. ▪ Multiple Transfer Mechanisms: AT&T will maintain the capability to accept all required data transfer mechanisms for data sets transferred from the government to the AT&T and will submit data to the government using the listed data transfer mechanisms unless an exception is approved by the relevant CO.
Direct Data Exchange	
Direct Data Exchange Mechanisms [J.2.9.2.1]	AT&T supports direct data exchange between its BSS and GSA Conexus based on the requirements captured in RFP Section G.5.3.2 using Web Services with commercial practices and standards and SFTP exchanged via a server operated by or on behalf of GSA.
Attachments via Direct Data Exchange [J.2.9.2.2]	AT&T also submits any BLOB attachments required in the definitions of the various data sets in RFP Section J.2.10.2. AT&T transfers these files separately via SFTP and names the files based on the template provided in RFP Section J.2.9.2.2. AT&T will not submit attachments with filenames that are not fully compliant with the specified template except as authorized. AT&T will package/compress large files using zip formats as appropriate.
AT&T's Website	
AT&T's Website [J.2.9.3]	Requirements for data transfer via the AT&T's web interface appear in RFP Section G.5.3.1.
Email	
Email [J.2.9.4]	When emailing data to the government, AT&T: ▪ Uses body text only for brief information (not to exceed 150 words) ▪ Uses attachments for longer data sets or for structured data ▪ Uses attachment formats that are compatible with one of the following – Microsoft Office (current version and two most recent prior versions) – PDF – Other formats as approved in writing by the relevant CO ▪ Encrypts attachments if required by the TO or the relevant CO ▪ Includes appropriate contract and TO identification information in the body and all attachments ▪ Submits directly to the POC specified by the OCO.
GSA Systems	
GSA Systems [J.2.9.5]	Data submitted by AT&T to GSA Systems is submitted as uploaded files in either: 1) the original format of the document, or 2) in CSV format, as defined for each deliverable specified as submitted via GSA Systems in RFP Section J.2.10.2.
Other Means as Agreed or Required in the TO [J.2.9.6]	The use of other means to transfer data must be approved in writing by the relevant agency CO or included in the TO.

3.10 Data Dictionary [J.2.10]

In addition to having a common understanding of how data will be exchanged and of the deliverables in which it will be provided, it is important to have a common understanding of the data field meanings and location within each data exchange. This facilitates compilation and interpretation of the data in support of contract management. Whether it is data receipt or delivery, AT&T's BSS is designed to support reference data sets specified in RFP Section J.2.10.2 using data transfer mechanisms as defined in RFP Section J.2.9. **Figure 3.10-1** depicts our EIS BSS CDIP-compliant data interchange flow and data transfer mechanisms.

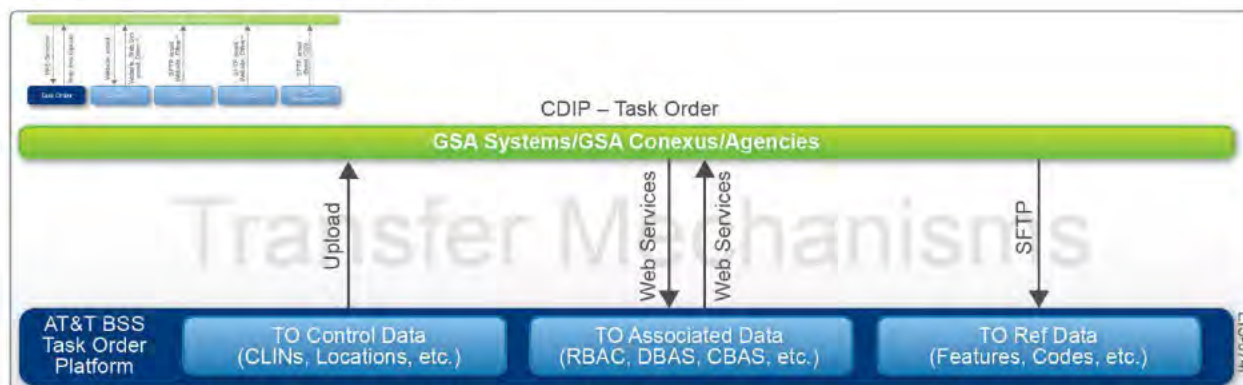


Figure 3.10-1. CDIP-Task Order Data Management Process Flow. Automated and highly secure transfer of TO data is fully compliant with EIS requirements and cover the three categories of data exchanged.

3.10.1 Common Data Requirements [J.2.10.1]

The CDIP first addresses common data requirements for the Data Dictionary, which provides additional instructions for specific fields for which GSA would like to provide special guidance and explanation. **Table 3.10-1** provides details of AT&T's compliance with the common data requirements of the data dictionary.

Table 3.10-1. CDIP Other Data Dictionary Requirements. AT&T fulfills 100% of the CDIP other data dictionary requirements.

Common Data Requirements [J.2.10.1]	
Extended Data Element Definitions [J.2.10.1.1]	All data elements are defined with technical specifications in RFP Section J.2.10.3. However, a few data elements require more detailed explanations and definitions. Those elements are defined in the subsections below.
Associated Government Fee [J.2.10.1.1.1]	Direct-billed customers: On a monthly basis, AT&T collects the AGF from our customers and remits to GSA as described in RFP Section G.4.6.
AGF Rate Structure [J.2.10.1.1.1.1]	AT&T understands and complies with the AGF Rate Structure governance
AGF Calculation [J.2.10.1.1.1.2]	AT&T understands and complies with the AGF Calculation process
Unique Billing Identifier [J.2.10.1.1.2]	AT&T understands and complies with the UBI specifications, requirements, and assignment processes as required by RFP Section J.2.10.1.1.2, item 2.

Common Data Requirements [J.2.10.1]	
UBI Specifications [J.2.10.1.1.2.1]	- The UBI is structured as two substrings separated by an underscore: Service Grouping ID_Component ID - AT&T will provide the UBI as per instructions in the Primary Data Element Dictionary. The UBI will contain only the single underscore and will be unique across the contract. It will never be reused.
UBI Process Requirements [J.2.10.1.1.2.2]	- AT&T creates and assigns the UBI for each installed service instance in compliance with the UBI Specifications as described in RFP Section J.2.10.1.1.2.1, even if there is only one member of the group AT&T provides the UBI to the government as part of the SOCN and all other deliverables where it is a listed data element as specified in RFP Section J.2.10.2 - For auto-sold CLINs and CLIN bundling (see RFP Section B.1.2.12), AT&T assigns UBIs to the base CLIN (including TUC), and to each associated auto-sold or component CLIN, and validates that the service grouping is the same on each - AT&T maintains the UBI assignment for the duration of the contract even if the service is later disconnected - AT&T applies logical grouping when constructing the service grouping.
Network Site Code [J.2.10.1.1.3]	- As a telecommunications provider, AT&T has an existing agreement with iconectiv and has long-standing processes surrounding interface with the Central Location Online Entry System (CLONES) database. AT&T will retain access to CLONES, at AT&T's cost, in support of EIS requirements. - AT&T will use the iconectiv CLONES database to derive the Network Site Code (NSC) for all locations associated with an order following the direction provided in RFP Section J.2.10.1.1.3(2) - As per existing processes, AT&T requests NSC from the iconectiv CLONES provider if the NSC for the location does not exist in the iconectiv CLONES database - AT&T will capture and store the NSC, billing, originating and terminating address information as applicable, and provide the same on all deliverables as required.

Order Types [J.2.10.1.1.4]: In order to understand the flow of updates within the inventory records, record level change controls are required. AT&T's system infrastructure design fully complies with the order type codes supplied by the government to be applied at the Header Level and Line Item Level within service orders. AT&T understands and complies with the Header and Line Item Level order type values detailed in RFP Section J.2.10.1.1.4. A summary of the order types is in **Table 3.10-2**.

Table 3.10-2. Order Types. Order type elements and definitions help assure customer needs are adequately and efficiently met.

Order Types [J.2.10.1.1.4]	
- Orders for New Services [J.2.10.1.1.4.1] - Orders to Change Existing Services [J.2.10.1.1.4.2] - Move Orders [J.2.10.1.1.4.2.1] - Change in Features [J.2.10.1.1.4.2.2] - Configuration [J.2.10.1.1.4.2.3] - Disconnect [J.2.10.1.1.4.2.4] - Change in Administrative Data [J.2.10.1.1.4.2.5]	- Order to Supplement or Update In-Progress Orders [J.2.10.1.1.4.3] - Order Cancellation [J.2.10.1.1.4.3.1] - Line Cancellation [J.2.10.1.1.4.3.2] - Update Specified Location [J.2.10.1.1.4.3.3] - Update Specified Features [J.2.10.1.1.4.3.4] - Update Specified Customer Want Date [J.2.10.1.1.4.3.5] - Update Specified Administrative Data [J.2.10.1.1.4.3.6] - Clarification of Line Items Being Updated [J.2.10.1.1.4.3.7]

Data Transaction Code [J.2.10.1.1.5]: For each data set exchanged between GSA and AT&T, whether it is ordering or another data set, a data_transaction_code element

will be included. This element will identify the specific data set. AT&T's systems will accept the element when GSA provides data to AT&T and will include the correct data transaction code in each data set submitted to GSA. AT&T will follow the predefined code included within the data set definitions of RFP Section J.2.10.2.

Data Consistency [J.2.10.1.2]: In addition, in order for government systems to execute repeatable processes, the data formatting of AT&T's deliverables must be consistent. As required in RFP Section J.2.10.1.2, AT&T will submit each data element in a consistent format.

Data Set Structure [J.2.10.1.3]: Table 3.10-3 provides details of AT&T's understanding and application of Data Set Structure.

Table 3.10-3. Data Set Structure. *Data set structure helps AT&T maintain consistent and quality data exchange.*

Data Set Structure [J.2.10.1.3]	
GSA Systems CSV Structure [J.2.10.1.3.1]	For all data sets submitted as CSV via GSA Systems, the data element order listed in RFP Section J.2.10.2 is used in structuring the table (i.e., the column order of the submitted table matches the specified field order). For data sets submitted with multiple rows of data, all data elements are included in each row even if unchanged from the previous row.
PSV Structure [J.2.10.1.3.2]	For all data sets submitted using PSV over SFTP, the data element order listed in RFP Section J.2.10.2 is used in structuring the PSV file (i.e., the column order of the submitted file matches the specified field order). For data sets submitted with multiple rows of data, all data elements are included in each row even if unchanged from the previous row.
XML and Web Services Structure [J.2.10.1.3.3] GSA Conexus XML Schema Definitions [J.2.10.1.3.3.1] GSA Conexus Web Services Definitions [J.2.10.1.3.3.2]	For all data sets submitted using XML over Web Services, the data is structured in accordance with the applicable XML Schema Definitions (XSDs), Web Services Definition Language (WSDL) documents, and associated documents provided by GSA. AT&T uses these schemas and documents in establishing Web Services connections with GSA Conexus.

3.10.2 Data Set Content [J.2.10.2]

GSA has provided detailed data set requirements in order to facilitate the exchange of data between GSA and AT&T. AT&T's system and deliverables supporting EIS are designed to fully comply with the requirements detailed in RFP Section J.2.10.2. To facilitate understanding of the requirements, GSA has organized the data sets into three groups: Primary Data is addressed in Table 3.10-4; Reference Data is addressed in Table 3.10-5; and TO Data is addressed in Table 3.10-6.

3.10.2.1 Data Sets: Primary Data [J.2.10.2.1]

AT&T understands and complies with the constructs defined for the primary data sets. The top portion of Table 3.10-4 provides definitions applicable to each column of the

primary data sets identified in the subsections of RFP Section J.2.10.2.1. The bottom portion of **Table 3.10-4** highlights the subsections.

Table 3.10-4. Primary Data. *Accepting and applying the content for Primary Data Sets enables AT&T to achieve consistency and quality of data exchange.*

Element Name	Value Requirement	Unique Value Level
- This is the actual element name, which will be used in the xml file for data sets transacted via Web Services - For data sets transacted via Secure FTP, this is the column heading - The Element Name value corresponds to element specifications in RFP Section J.2.10.3.	- Always: AT&T will provide the correct value for the element on all submissions when the Value Requirement is Always - If Applicable: AT&T will supply the correct value for the element on all submissions when the Value Requirement is If Applicable - Either/Or: AT&T will supply the correct value for only one of the data elements labeled and will apply the specific requirements for that data set in choosing which to supply. For data transferred via Web Services, the data field can be omitted. In all other cases, all data element fields will be present even if empty.	- AT&T follows the guidance in this field, which indicates if the value can vary with each line item in the data set or if the data set is only permitted to have the same value for each line item - If the Unique Value Level is not provided for a data set, all data elements in that data set may vary by line item.
Data Set		Transaction Code
Administrative Change Order [J.2.10.2.1.1]		SO
AGF Detail [J.2.10.2.1.2]		AGFD
AGF Electronic Funds Transfer Report [J.2.10.2.1.3]		ATR
Billing Adjustment [J.2.10.2.1.4]		BA
Billing Invoice (BI) [J.2.10.2.1.5]		BI
Direct Billed Agency Setup [J.2.10.2.1.8]		DBAS
Dispute [J.2.10.2.1.9]		D
Dispute Report [J.2.10.2.1.10]		DR
Firm Order Commitment Notice [J.2.10.2.1.11]		FOCN
Inventory Reconciliation [J.2.10.2.1.12]		IR
Monthly Billing Information Memorandum [J.2.10.2.1.13] - Unless otherwise specified by a TO, AT&T may use its standard commercial report format for this deliverable so long as detail is sufficient to: - Uniquely identify the associated BI - Clearly communicate key elements in the BI that require explanation or background information - Provide an overview of AT&T's reasoning, explanation, and/or background information.		n/a
Service Level Agreement Report [J.2.10.2.1.14]		SLAR
Service Order [J.2.10.2.1.15] - AT&T will collect the minimum data set defined in RFP Section J.2.10.2.1.15 - AT&T will also collect from the government all order information needed to complete all other deliverables. With OCO concurrence, AT&T may further define how that data is provided.		SO
Service Order Acknowledgement [J.2.10.2.1.16]		SOA
Service Order Administrative Change [J.2.10.2.1.17]		SOAC
Service Order Completion Notice [J.2.10.2.1.18]		SOCN
Service Order Confirmation [J.2.10.2.1.19]		SOC
Service Order Rejection Notice [J.2.10.2.1.20]		SORN
Service State Change Notice [J.2.10.2.1.21]		SSCN
SLA Credit Request [J.2.10.2.1.22]		SLACR

Element Name	Value Requirement	Unique Value Level
SLA Credit Request Response [J.2.10.2.1.23] ▪ AT&T will use our commercial format dispute response		n/a
Tax Detail [J.2.10.2.1.24]		TAX
Trouble Management Incident Performance Report [J.2.10.2.1.25] ▪ AT&T will provide a Trouble Management Incident Performance Report, which is compliant with RFP Section G.8.5.2.4		n/a
Trouble Management Performance Summary Report [J.2.10.2.1.26] ▪ AT&T will provide a Trouble Management Performance Summary Report, which is compliant with RFP Section G.8.5.2.3		n/a

3.10.2.2 Data Sets: Reference Data [J.2.10.2.2]

Data elements in **Table 3.10-5** are transferred from GSA to AT&T and will always include values for all data elements.

Table 3.10-5. Reference Data. AT&T acknowledges and applies the reference data sets.

Element Name	Data Transaction Code	Element Name	Data Transaction Code
Access Circuit Type [J.2.10.2.2.1]	CKTTYP	Dispute Reason [J.2.10.2.2.17]	DRSN
Access Framing [J.2.10.2.2.2]	AFRAM	Dispute Status [J.2.10.2.2.18]	DSTUS
Access Jack Type [J.2.10.2.2.3]	JCKTYP	KPI AQL Type [J.2.10.2.2.19]	KPIAO
Access Provisioning [J.2.10.2.2.4]	APROV	KPI Location Qualifier [J.2.10.2.2.20]	KPILQ
Account Type [J.2.10.2.2.5]	ACTTYP	KPI Measurement Unit [J.2.10.2.2.21]	KPIMU
Active/Inactive [J.2.10.2.2.6]	ACTINA	KPI Service Level Qualifier [J.2.10.2.2.22]	KPISLQ
Adjustment Outcome [J.2.10.2.2.7]	ADJOUT	KPI Unit Code [J.2.10.2.2.23]	KPIUC
Adjustment Reason [J.2.10.2.2.8]	ADJRSN	Line Coding [J.2.10.2.2.24]	LNECD
Agency Bureau Code [J.2.10.2.2.9]	ABCODE	LOA Dependencies [J.2.10.2.2.25]	LOADEP
Allowable Tax [J.2.10.2.2.10]	ALLTAX	Order Rejection [J.2.10.2.2.26]	ORDREJ
Bandwidth [J.2.10.2.2.11]	BANDW	Order Type: Header Level [J.2.10.2.2.27]	ORDHRD
		Order Type: Line Item Level [J.2.10.2.2.28]	ORDITM
Charging Frequency [J.2.10.2.2.13]	CRGFRQ	Primary Interchange Carrier (PIC) [J.2.10.2.2.29]	PIC
Charging Unit [J.2.10.2.2.14]	CRGUNT	Service [J.2.10.2.2.30]	SVC
Country [J.2.10.2.2.15]	CNTRY	True/False [J.2.10.2.2.31]	TRUFLS
Data Transaction Type [J.2.10.2.2.16]	DTT	Yes/No [J.2.10.2.2.32]	YESNO

3.10.2.3 Data Sets: Task Order Data [J.2.10.2.3]

Table 3.10-6 describes AT&T's process, structure and content for TO Data exchange. AT&T submits TO Data to GSA via Data Transfer Mechanisms defined in RFP Section J.2.9 and following the structure provided in RFP Section J.2.10.2.3. All data elements will be present even if empty. A valid value will always be provided with the exception of: Task_order_modification_number and Stop_date which are only required if applicable.

Table 3.10-6. Task Order Data. *AT&T strictly complies with all TO data requirements.*

Data Sets: Task Order Data [J.2.10.2.3]	
TO CLINs Awarded [J.2.10.2.3.1]	- AT&T will provide the TO CLINs Awarded deliverable when not all CLINs for a service have been awarded to AT&T - Contains only the CLINs that were awarded to AT&T within the TO - AT&T submits the data in CSV format, containing the data elements in the table at RFP Section J.2.10.2.3.1, via GSA Systems.
TO Customer Requirements Document Set [J.2.10.2.3.2]	AT&T submits the following documents in their original formats to GSA Systems: - Final version of the RFP, RFQ, or equivalent document issued by the agency, inclusive of all amendments - Any other documents the customer uses to support its requirements - Final TO Proposal Volumes - TO Award Document.
TO Financials [J.2.10.2.3.3]	The table includes a separate line for each performance period fiscal year (FY) covered by the TO. This data is submitted in CSV format to GSA Systems and contain the data elements in the table at RFP Section J.2.10.2.3.3.
TO Country/Jurisdictions Awarded by Service [J.2.10.2.3.4]	Contains all countries/jurisdictions awarded by service to AT&T within the TO. This data is submitted in CSV format to GSA Systems and contains the data elements in the table at RFP Section J.2.10.2.3.4.
TO Key Performance Indicators [J.2.10.2.3.5]	Contains all KPIs specific to the TO where: 1) the KPIs are not in the contract, or 2) the TO overrides the contract KPI. This data is submitted in CSV format to GSA Systems and contain the data elements in the table RFP Section J.2.10.2.3.5.
TO Locations Awarded by Service [J.2.10.2.3.6]	Contains customer locations by service awarded to AT&T within the TO for those services not awarded at the country/jurisdiction level. Services awarded at the country/jurisdiction level are omitted from this deliverable. This data is submitted in CSV format via GSA Systems and contain the data elements in the table at RFP Section J.2.10.2.3.6.
TO Officials [J.2.10.2.3.7]	Contains all OCOs and CORs (if applicable) associated with the TO. This data is submitted in CSV format via GSA Systems and contain the data elements in the table at RFP Section J.2.10.2.3.7.
TO Service Awarded [J.2.10.2.3.8]	Contains all services awarded to AT&T within the TO. This data is submitted in CSV format via GSA Systems and contain the data elements in the table at RFP Section J.2.10.2.3.8.

3.10.3 Data Element Specifications [J.2.10.3]

In order to fully implement a supportive data exchange between GSA and AT&T, the structure of the data fields included in the data sets need to be defined. Each party must understand the field description, type, length, and edit mask. GSA has defined these parameters in RFP Section J.2.10.3, and AT&T's deliverables conform to and comply with the requirements of the following subsections:

- Primary Data Element Dictionary [J.2.10.3.1]
 - Interpreting the Primary Data Elements List [J.2.10.3.1.1]
 - Primary Data Element List [J.2.10.3.1.2]
- Reference Data Element Dictionary [J.2.10.3.2]
- Interpreting the Reference Data Elements List [J.2.10.3.2.1]

▪ Reference Data Element Dictionary Table [J.2.10.3.2.2]

CDIP Conclusion: A well-defined, well-followed, and change-controlled data infrastructure will allow GSA and AT&T to exchange data sets throughout the life of the EIS contract in support of the agencies using the contract. GSA has provided the Common Data Requirements, Data Set Content, and Data Element Specifications, and AT&T provides a high-quality system, which fully complies with all associated requirements.

Management Volume Summary: In support of GSA's vision to have EIS become the agency preferred strategic sourcing vehicle for telecommunications services, we have provided this comprehensive, fully compliant proposal. Throughout this volume and the referenced appendices, we explained our approach to bring our people, processes, and tools together to effectively support GSA and all agencies. This management volume described how we will provide the following three critical management components required for successful EIS contract execution:

1. **Operational Success** enabled by an in-place, customer-focused CSO infrastructure
2. **Agency Usage** facilitated through highly secure portal and BSS that facilitate, and
3. **Continuity** of knowledge delivered through program understanding and leadership that delivers

GSA and all agencies can be confident that AT&T has the management infrastructure to effectively provide industry leading services and support on the EIS contract.



Figure 3.10.3-1. Elements for Success. AT&T's management foundation directly supports GSA's vision for EIS.



General Services Administration (GSA)

Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

GS00Q17NSD3000
Appendix A — Program Management Plan

APPENDIX A — PROGRAM MANAGEMENT PLAN (PMP) [L.30; L.30.2.1; M.2.2 (3 OF 3); G.9.4; C.3; H.10; H.35; D; F]

GSA states in the solicitation that one of its goals is *“to make...[EIS] contracts as flexible and agile as possible to meet and satisfy the widely differing requirements of the federal agencies both now and for the next decade and beyond.”* The EIS contract is a significant component of GSA’s broader NS2020 vision, and the success of EIS will help GSA to bring the benefits of its portfolio management to the federal government.

This Program Management Plan (PMP) details our methods and implementation plan for managing EIS to meet GSA’s goals, employing structured, repeatable project management methodologies to manage scope, schedule, and risk, and to effectively allocate resources required to achieve the mission. This plan incorporates lessons learned over decades of collaborating with GSA to provide telecommunications services to the federal government.

This comprehensive PMP, which is fully compliant and will remain in effect throughout the duration of the contract, includes how we communicate effectively with GSA and agencies and acknowledges we are accountable for our technical performance on the contract [G.9].

AT&T’s PMP describes our processes and abilities to responsively plan, control, and execute our activities under the EIS contract. The PMP incorporates the following program management functions [G.9.1]: program control, planning at the program level, planning at the agency level, AT&T performance, resource management, revenue management, reporting and reviews, and senior-level communications. Details required to address our approach for transition, resources, quality assurance (QA), risk management, business support systems solution and methodologies, and our PMP organizational structure are all contained within **Appendix A, Section A-1**. A summary of our EIS PMP is provided in **Table A-1**.

Table A-1. EIS PMP Summary. *This Program Management Plan (Appendix A) is organized in accordance with (IAW) RFP Section L and Section G.9.4 for ease of evaluation and understanding.*

Section	Title	Content
A-1	Contract Management Requirements	PMP introduction and listing of government dependencies and assumptions required to properly execute EIS
A-2	Description of Service Solution	AT&T methodologies used to comply with service ordering, billing, inventory management, and service management requirements.
A-3	Draft Program Management Schedule	Identification of major milestones and activities for: (1) BSS testing, (2) BSS Federal Information Security Management Act (FISMA) compliance, and (3) Authority to Operate (ATO). The level of detail will vary for each

Section	Title	Content
		of the above milestones and will address major activities within a timeline consistent with EIS requirements.
A-4	Draft Transition Management Approach	Detailed AT&T approach to the project management of transition
A-5	Resource Plan	Definition of our approach to financial resources for budgeting, tracking, and controlling costs and human resources to retain qualified personnel. Also includes our system for managing hardware (HW) and software (SW) assets.
A-6	Quality Assurance Program	AT&T implementation, review, and enforcement of Acceptable Quality Levels (AQL), SLAs, and customer support services.
A-7	Key Personnel & Organizational Structure	Management organization to successfully deliver EIS and key personnel qualifications
A-8	Risk Management	Description of the AT&T risk management methodology, including identification and mitigation approach.
A-9	Information Systems (BSS)	Overview of security plan to prevent unauthorized access.
A-10	Additional Elements	Description of security, reports, and deliverables
A-11	Summary	PMP Summary

A-1 Summary of Contract Management Requirements, Including Government Dependencies and Assumptions [L.30.2.1(1); G.9.4(1)]

Certain dependencies and assumptions underlay AT&T's technical and management approach to delivering EIS in the manner described in this proposal. **Table A-1-1** summarizes AT&T's dependencies regarding government roles/actions and enumerates basic assumptions in these areas.

Did You Know?

AT&T has processed 190,000 orders on the Networkx contracts, servicing 215 individual sub-agencies across 48 federal agencies.

Table A-1-1. Assumptions and Dependencies. AT&T is dependent on the actions of GSA, agencies and to enable effective support under EIS.

Area	Dependencies and Assumption	Assumption (A) or Dependency (D)	Dependent On
TOs	Provide appropriate documentation for Government Furnished Information (GFI) and Government Furnished Equipment (GFE) are an ordering agency responsibility in TO requests	D	Ordering Agencies
TOs	Support badging of staff/facility access as needed for installation and maintenance of equipment, or to meet specific EIS or TO requirements are an ordering agency responsibility	D	Ordering Agencies
Contract/TOs	Arrange for constructive participation /cooperation of outgoing contractors	D	GSA
Contract/TOs	Provide access to government facilities (as needed) to support required inventory management	D	Agencies
Contract/TOs	Make available EIS CO, OCO, COR to participate in training (as needed/appropriate)	D	GSA, Agencies
Contract/TOs	Provide timely approval of TO project plans	D	Agency OCO
Contract/TOs	Include valid data on orders	D	Agency OCO
Wiring/Circuits	Government to provide physical access to facilities to AT&T technicians for installation of access circuits and	D	Ordering Agencies

Area	Dependencies and Assumption	Assumption (A) or Dependency (D)	Dependent On
	premise wiring for delivery of services is an ordering agency responsibility		
Site, I&T Services	Government to provide access to facilities for pre-installation site surveys, and installation, maintenance and upgrades of premise equipment required for service delivery is an ordering agency responsibility	D	Ordering Agencies
Device Storage	Government to provide a secured storage and floor space, power and HVAC consistent with premise-installed Service Enabling Devices are ordering agency responsibilities	D	Ordering Agencies
Unique Transition Requirements	Any unique needs to support a project transition will be identified in the Transition Plan is an ordering agency responsibility	D	Ordering Agencies
Local Contacts	Local Government Contacts (LGC) are available to coordinate services at Customer Agency locations is an ordering agency responsibility	D	Ordering Agencies
Transition	Agencies will develop a transition plan and identify a transition manager	D	Agencies
Transition	Agencies are responsible for validating inventory accuracy	D	Agencies
Transition	Sufficiently skilled resources are available to execute TOs in support of a timely and orderly transition	D	Agencies
Transition	All outgoing contractor staff to provide timely data to incoming staff	D	GSA
Transition	Government to assist agencies for Fair Opportunity discussions and ordering	D	GSA
Testing	For the purposes of developing our draft BSS test plan and schedule, we assumed certain review and response times by GSA at each major stage of testing and approval.	A	GSA
Testing	Catalog will not be included as part of BSS Testing	A	GSA
Training	When training is provided via internet or remote means, the government provides the students the necessary computers, and internet access needed.	A	GSA, Agencies
Submission	AT&T is providing the completed Submission Matrix in the AcquServe portal.	A	GSA
EIS Verification and Testing	We assume that the correct name of the service within the "Colocated Hosting Service" service area is "Colocated Hosting Service" and not "Data Center Service".	A	GSA
Training	Per RFP requirements, AT&T provides EIS training to government users at no additional cost to the government. However, when training is provided via internet or remote means, AT&T assumes the government provides the students the necessary computers, and internet access needed	A	GSA
Contractor Data Interaction Plan	In support of future task orders, AT&T assumes that GSA will work with AT&T to adjust the XML schema to accommodate any agency-specific needs for which schema updates would be required.	A	GSA
Security of BSS	AT&T will support GSA in maintaining the risk assessment for our BSS	A	GSA

A-2 Summary Description of Service Solution [L.30.2.1(2); G.9.4(2)]

Our CSO supports GSA's requirement for a set of program-tested processes, standards, and a disciplined approach to support the EIS service areas of Service Ordering, Billing, Inventory Management, and Service Management (i.e., customer service and service assurance). AT&T's in-place infrastructure, coupled with our highly secure web portal and BSS (Systems), provide a structure and design that is both customer focused and user friendly. Access to each of these areas is primarily through the AT&T Business Support Systems (BSS), which is managed with the direction of our EIS CSO.

Business Support Systems (BSS). AT&T facilitates agency usage and supports data exchange communications via our BSS. This includes data exchanges with GSA Conexus as well as our Business Center web portal. Designed with the end-user in mind, our portal, shown in **Figure A-2-1**, provides customer access to Government Center (shown in green), which is being enhanced to support the unique data and reporting requirements of EIS. AT&T Business Center is the primary government access point for EIS services and AT&T's BSS. This portal is provisioned with two-factor authentication and role based access. The Contractor Data Interaction Plan provided in **Section 3** of our Management Volume response details our specific and effective approach to comply with the requirements of RFP Section J.2.



Figure A-2-1. AT&T Portal and BSS. GSA and Agencies receive customer access that is highly secure, intuitive, and versatile between platforms.

The following subsections describe AT&T's methodology to comply with the general and functional requirements for Ordering, Billing, Inventory, and Service Management.

A-2.1 Methodology to Comply with Service Ordering Requirements [L.30.2.1(2); G.9.4(2)]

AT&T complies with all ordering requirements as described in RFP Section J.2.4 Ordering and Section G.3.3 Ordering Services. Our methodology combines people, processes, and tools. We provide a dedicated contract modification team to support

both GSA and agency Task Order modification needs. In addition, we provide a dedicated ordering team to support receipt, assessment and processing of government requests, as well as processes to assist and respond to customer requirements to help validate order inputs. We also have tools such as Government Center, eBonding if needed for TOs, and APIs for gathering order data.

Ordering typically starts with a Task Order (or in some cases a purchase card order). Our dedicated Task Order Management team reviews each submitted TO to certify that the submission contains all required service data elements (e.g., CLINs, Agency Hierarchy Codes, etc.). If anything needs to be added to the TO before final execution, it is negotiated with the Agency CO. If any Task Order or general contract modifications are needed, those modifications are also managed by AT&T's TO Management Team. After the TO is executed, the TO Management Team uploads the TO and any associated documentation (RFPs, our response, pricing files, etc.) into our highly secure TO repository and in their original format. On a monthly basis, AT&T runs the various deliverable reports required at the TO level and provides them to the government. Service Order data that is captured from the TO is populated in our Service Ordering systems and reflected back to GSA via the various order notifications. Notifications are also visible to agency customers via our Government Center order management application. Additional details of our ordering solution and methodology in

Section 1.1.1. Table A-2.1-1 highlights AT&T's compliance with ordering requirements.

Table A-2.1-1. Compliance with Ordering Requirements. *CSO Ordering personnel satisfy all general and functional ordering requirements in support of GSA and Agency customers.*

General Ordering Processes	
- AT&T responds in a timely fashion to agency RFPs/RFQs and provides proposals and/or quotes - We accept, validate, and complete orders in association with all order requirements - AT&T obtains all needed information to deliver services based on the order and obtaining supplemental information through other sources such as site surveys - We accept a Letter of Authorization (LOA) from GSA giving the agency authority to place order under the EIS contract - AT&T supports all order types including moves, changes, cancels, and disconnects - We provide the required order acknowledgements and notifications	
Functional Ordering Processes (regarding placement, acceptance, and handling terms)	
Agency Hierarchy Code (AHC)	The Ordering Contracting Officer (OCO) provides an authorized and registered AHC for each TO. The AHC is tracked for all services for the life of that service on each order. Because the government does not pay for services associated with an AHC not registered to the TO, AT&T: validates that each task order has an AHC, validates that each order line item has an AHC and rejects any order submitted without an AHC for each line item, verifies the AHC for each TO Contract Line Item Number (CLIN) is the AHC provided by the OCO, validates the content of the AHC, if required by the TO, and confirms that changes in the AHC do not interrupt the associated services

General Ordering Processes	
Auto-Sold CLINs	Some services include other CLINs that may automatically be included with the original service order (e.g., additional storage included with web-based presentation replay). AT&T includes these Auto-Sold CLINs in the proposal or quote just as if they had been explicitly requested in the order. All Auto-Sold CLINs are listed in the notifications and deliverables associated with the order. When new Auto-Sold CLIN additions are added, AT&T issues new Service Order Completion Notices (SOCN) as applicable.
Customer Want Date	Customer Want Date (CWD) refers to the customers' desired installation date. AT&T does not issue the SOCN nor begin billing prior to the CWD unless the order specifies that early installation is acceptable. If the time between the order and the CWD is greater than the defined provisioning interval for the service as described in RFP Section G.8.2.2, the servicing provisioning SLA is waived for that service on that order.
Service Order Completion Notification (SOCN)	AT&T issues a SOCN no later than (NLT) three days after the completion of each service.

A-2.2 Methodology to Comply with Billing Requirements [L.30.2.1(2); G.9.4(2)]

The CSO is committed to issuing orders accurately, which leads to producing a quality bill. AT&T complies with all billing requirements as described in RFP Sections J.2.5 and G.4. We have designed EIS billing process and system flows to enable us to validate that line items invoiced contain the same key data points (i.e., AHC, ASRN, UBI) as those in the customer order and on the SOCN. This is achieved through our biller which supports flexible solutions that are designed to meet large custom contracts. The GSA and agencies are fully supported with highly secure, user-friendly Government Center invoice tools and processes that allow invoices, disputes, and payments to be tracked and completed in a timely, accurate manner. If a dispute should arise, it is quickly resolved by a team of billing associates supporting the EIS program.

Table A-2.2-1 highlights AT&T's compliance with general and functional requirements in support of GSA and agency billing processes. Additional details of our billing solution and methodology are in **Section 1.1.2**.

Table A-2.2-1. Compliance with Billing Requirements. GSA and agency customers are supported by billing tools and personnel which comply with all general and functional requirements.

General Billing Processes
- AT&T adheres to the government's defined billing cycle, which runs from the first through the last day of the calendar month - AT&T checks that the Unique Billing Identifier (UBI) reported on billing deliverables match the UBI included on all Service Order Completion Notices (SOCN) - For all billing deliverables, AT&T provides the CLIN and all associated Individual Case Basis (ICB) data elements for each line item and certifies that the CLINs match those on the SOCN for each respective order - AT&T calculates all Associated Government Fees (AGF) as enumerated in RFP Section J.2.10.1.1.1 AGF Rate Structure and provides the AGF as a data element in our billing deliverables. For TOs with direct billing, AT&T collects the AGF and transfers it to GSA - For proration purposes, AT&T calculates: daily charge = the monthly recurring charge/30; billable days = days in month — (start day — 1) but notes that if billable days < 30, proration does not apply; billable amount = daily charge x billable days. When a service change order effects a price change during a billing cycle, AT&T treats

General Billing Processes	
the change as connected events with a previous service price and a new service price start with proration applying to both. - AT&T calculates charges and use for service price, prorating, taxes, fees, and surcharges to the sixth decimal and rounds according to those standards described in RFP Section J.2.5.1.6.2 Rounding Standards. This sixth decimal standard is also applied to calculating summary data of cost components and to the totaling of the entire submitted bill. - AT&T fully complies with all requirements for handling taxes, fees, and surcharges as detailed in RFP Sections G.4.11 Taxes, Fees, and Surcharges, H.14 State and Local Taxes, and H.23 Fees and Surcharges. AT&T applies taxes to each taxable line item as an aggregated total per billing line item and provides a detailed composition of the aggregated tax on the Tax Detail deliverable. - AT&T submits billing deliverables to GSA in accordance with RFP Section J.2.5.2 and according to TO billing level and billing type - AT&T submits the Billing Invoice, Tax Detail, Monthly Billing Information Memorandum, Billing Adjustment (if applicable), AGF Detail, and the AGF Electronic Funds Transfer Report deliverables NLT the 15th business day of each month according to the appropriate transfer mechanism (e.g., SFTP). If corrective actions are identified after payment, AT&T submits a Billing Adjustment.	
Functional Billing Processes	
Adjustments	If and when it is necessary to adjust a bill, AT&T complies with the adjustment processes detailed in RFP Section J.2.5 Billing and applies the adjustment to the next available bill. If there is a dispute, AT&T follows the dispute process described in RFP Sections G.4.4 Disputes and J.2.6 Billing and Disputes.
Monthly Billing Information Memorandum	As needed, AT&T provides a Monthly Billing Informational Memorandum to accompany the monthly delivery of billing files. This memorandum is a narrative accounting of the changes in billing, changes in formats, and new services added to the billing and an explanation of the issues pertaining to balancing charges.

A-2.3 Methodology to Comply with Inventory Management Requirements [L.30.2.1(2); G.9.4(2)]

AT&T complies with all inventory management requirements. [REDACTED] the inventory management system and processes to specifications provided in RFP Sections J.2.7 and G.7. [REDACTED]

Table A-2.3-1

[REDACTED] in support of GSA and agency inventory management processes. Additional details of our inventory solution and methodology are in **Section 1.1.6**.

[REDACTED] within one business day of the issuance of the SOCN. Updates include all additions, deletions or changes to the EIS services being provided to GSA and Agencies. [REDACTED]

to the government customer during the contract and for three years following the expiration or termination of the contract. To certify that EIS inventory data is complete and accurate,

Table A-2.3-1. Compliance with Inventory Management Requirements.

General Inventory Management Processes (Regarding Processes, Deliverables, and Data Exchange Requirements)	
Functional Inventory Management Processes	
EIS Inventory	
EIS Services	
Inventory Reconciliation (IR)	

A-2.4 Methodology to Comply with Service Management Requirements [L.30.2.1(2); G.9.4(2)]

AT&T complies with all service management requirements as described in RFP sections J.2.8, G.6, and G.8. Service management includes Service Level Management (**Section 1.1.7**) and Service Assurance (**Section 1.1.4**, which includes the customer support office and technical support), Supply Chain Risk Management (**Appendix B**), and Trouble Ticket Management (**Section 1.1.5**.)

The CSO is the operational engine driving AT&T's EIS performance and functions as the primary interface with GSA and EIS customer agencies worldwide. CSO functional groups are organized along administrative lines similar to those used on Networx and

have clearly defined areas of responsibility that all work together providing an effective, user-friendly EIS experience for GSA and customer agencies. We have dedicated SLA managers who support the various reports required — using customized and standard tools to generate the reports and to support analysis for continuous improvement opportunities. EIS customers also receive customer and administrative support from implementation and service teams backed by AT&T's global support organizations. AT&T pairs dedication to customer service with an equally rigorous commitment to service assurance via metric-driven Service Level Agreements (SLA) and consistent performance reporting. AT&T complies with the service-specific SLAs to meet or exceed service-specific performance levels, consistent with the appropriate technical requirements. AT&T also complies with service-independent SLAs. We approach Trouble Handling not only as a means to document and to resolve customer issues, but also to manage our actual service levels in comparison to the planned service levels, and to identify areas for improvement. **Table A-2.4-1** highlights our compliance with general and functional requirements in support of GSA and agency service management processes.

Table A-2.4-1. Compliance with Service Management Requirements. *AT&T Service Management and Service Assurance personnel satisfy all general and functional requirements in support of GSA and Agency customers.*

General Service Management and Service Assurance Processes	
Service Level Management	AT&T consistently measures each applicable SLA according to its definition, tracking its performance relative to each associated KPI as enumerated in RFP Section G.8.3.1. If an SLA is missed, the government issues a credit request within six (6) months of the SLA failure. AT&T reviews these requests and responds within 30 days and (if approved) issues the credit within two billing cycles. AT&T submits all deliverables and data sets associated with the SLA reporting process (e.g., SLA Report, Trouble Management Performance Summary, and the Trouble Management Incident Performance Report) and the SLA credit process (i.e., SLA Credit Request Response) in accordance with the frequency and transfer mechanisms described in RFP Section J.2.8.3. AT&T meets all SLA requirements as enumerated in RFP Section G.8.2 including those for delivering the service, maintaining the service at specified AQL, measuring the KPIs, compliance reporting, and issuing requested credit when performance fails to meet objectives. Processes for measuring and sampling are described in the Quality Control (QC) section of our PMP. AT&T submits SLA management reports (e.g., SLAR, SLACR, Trouble Management Performance Summary and Incident Performance Reports) via the AT&T Government Center and via direct data exchange in accordance with requirements detailed in RFP Section G.8.5. In the unlikely event that AT&T fails to meet a contractual or TO-defined SLA, we shall respond to customer requests for credits to the GSA or the government agency of record according to RFP Section G.8.4.
Functional Service Management and Service Assurance Processes	
Customer Support	The AT&T CSO is the primary interface for government entities interested in using the EIS contract. We identify the organizational structure components of our CSO, which is responsible for supporting the transactions, service, and implementation activities with the government. The CSO provides training and communicates with users across multiple

General Service Management and Service Assurance Processes	
	channels including a toll-free number, email, web-based collaboration tools, and agency-dedicated Customer Service Representatives (CSR). AT&T's CSO is located in Oakton, VA and will be fully operational for EIS support within 30 days of NTP.
Supply Chain Risk Management (SCRM)	The AT&T SCRM Plan outlines our approach to mitigate and reduce supply chain risks such as counterfeit and illegally modified products. Our SCRM Plan addresses supply chain risk holistically across five phases: design and engineering, manufacture and assembly, distribution and warehousing, operations and support, and disposal and return, while also identifying any supporting infrastructures beyond the system boundaries. Details are provided in Appendix B .
Trouble Ticket Management	AT&T performs trouble ticket management in accordance with the government's general and reporting requirements. AT&T provides a trouble ticket for any reported or discovered service issue, provides status updates, and provides the resolution to the initiator. AT&T provides trouble ticket management, escalation, and resolution with 24x7 accessibility within the timeframes specified in RFP Section G.8. According to priority, AT&T first restores any Telecommunications System Priority (TSP) restoration coded service and then escalates issues according to our PMP. AT&T provides query, sorting, exporting, and saving capabilities across PDF/CSV or standard/structured file formats by any field or combination of formatted fields for each trouble ticket record. In the unlikely event of a service outage, AT&T supports requested credits based on this record of trouble reporting information. Within five days upon request from the GSA Program Management Office (PMO) or agencies, AT&T delivers archived trouble and complaint data.

A-3 Draft Program Management Schedule [L.30.2.1(3); G.9.4(3)]

GSA will receive expedited transition of services due to the structured AT&T process for achievement of early ATO. The draft Program Management Schedule focuses on steps required to establish the program and features a transition plan along with comprehensive BSS testing plan, FISMA compliance processes, and

schedule controls. Combining past experience, details provided in the EIS RFP, and known external factors, AT&T has created a draft Program Management Schedule. This translates to a low risk solution and a customer schedule-driven transition to benefit GSA and the agencies. This schedule, depicted in **Figure A-3-1**, highlights our

Did You Know?

AT&T embedded the principles of GSA's "5 Pillars of Success" for migration into our planning and development process when we drafted our program management schedules by accounting for agency involvement, transition planning, phased approaches, early support, and reporting transparency.

contractually-required

deliverables, milestones

described in the contract,

and incorporates

assumptions regarding

durations of activities.

While making the duration

assumptions, AT&T has

kept in mind the need for

EIS to be enabled as

quickly as possible to support agency transitions in advance of expiration dates of

Networx and LSA contracts. To engage with transition implementations, we must first

achieve ATO. **Figure A-3-2**

details the specific steps

required to achieve ATO as

quickly as possible. We will

engage some of the same

resources who supported

Networx BSS verification, as well

as corporate resources skilled in

system test execution. We will

apply consistent project and

schedule management

methodologies and techniques in

order to mitigate schedule delay

risk. We assume that BSS

verification testing will take 90

days based upon the volume of services that we are proposing. We also assume that

GSA's review of Security Assessment and Authorization (A&A) will take 90 days. AT&T

will prepare and maintain required documentation in parallel to BSS verification testing

so that we are ready to deliver artifacts as soon as the BSS tests are complete.

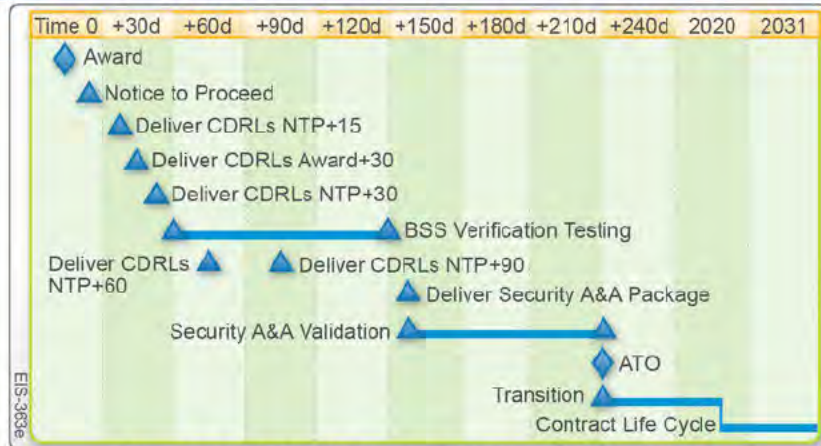


Figure A-3-1. Draft Program Management Schedule.
GSA receives expedited transition of services due to the structured AT&T process for achievement of early ATO.

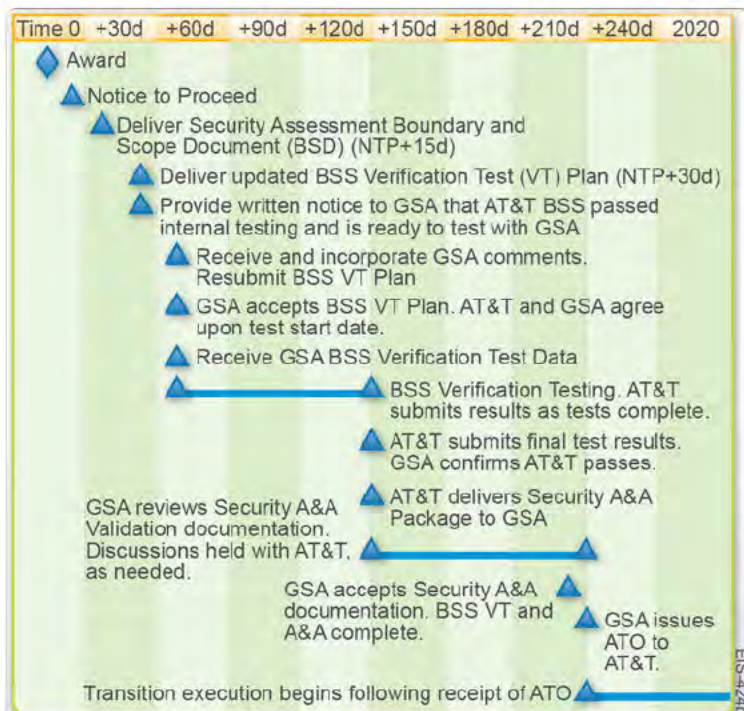


Figure A-3-2. Schedule to Achieve ATO. GSA issues ATO only after successful completion of BSS verification testing and security A&A.

AT&T works with GSA stakeholders to refine requirements and adjust the EIS schedule as appropriate to account for varied milestones and to meet a timely delivery.

BSS Testing: AT&T demonstrates end-to-end functionality (ordering, inventory, billing/dispute handling, ticketing, catalog, and SLA management) on our BSS platform.

Figure A-3-3 presents an AT&T estimate of the schedule to perform all of the testing required for all services awarded to demonstrate acceptability. Our BSS testing approach is built within our BSS test production environment, uses test data provided by GSA, embeds a feedback loop for results verification (and retesting if needed), and uses the expertise of our Networkx subject matter specialists to assist, and support BSS functional testing. Details of

this plan are provided in

Appendix C. We estimate

actual testing will take up to 90

calendar days due to

robustness of the BSS services

AT&T is proposing.

FISMA Compliance: Our support team includes information systems security subject matter specialists with experience achieving FISMA compliance. The schedule in

Figure A-3-4 shows the major milestones to achieve FISMA compliance, including completion of the System Security Plan (SSP), the completion and submission of the

Security A&A package, and

GSA issuance of ATO. FISMA

details at service levels are

provided in **Appendix D.** For

the purposes of this draft

schedule, AT&T assumes that

GSA will require 90 days to

review the AT&T security

package.

Schedule Controls: AT&T manages schedules on EIS through a series of controls

including milestone and program reviews intended to track and confirm progress versus

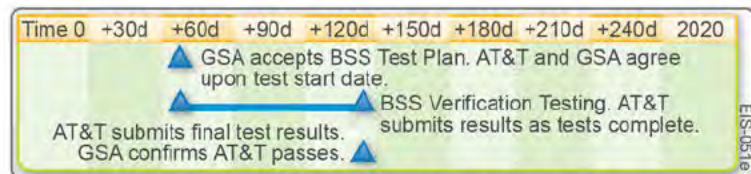


Figure A-3-3. BSS Testing and Validation Schedule.
GSA benefits from AT&T's lessons learned on the Networkx transition to complete BSS testing and verification.

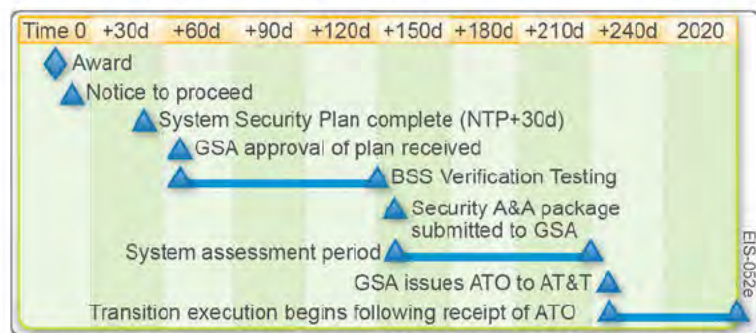


Figure A-3-4. FISMA Approval Timeline. *FISMA compliance is achieved before the launch of full-scale EIS transition activities.*

the baseline schedule. As changes arise such as adjustments in stakeholder requirements, execution experience, delays, or accelerated completions, change control processes will allow for schedule adaptation, escalation, or other necessary activity to occur. Through the process of controls, we will be able to forecast staffing needs, track performance, and enable effective program management.

A-4 Draft Transition Management Approach, Including Project Management Process, Procedures, and Tools To Meet the Transition Requirements in Section C.3 [L.30.2.1(4); G.9.4(4); C.3-C.3.3.4]

GSA's transition approach will be supported by the experience we have garnered transitioning Networkx and other contracts, which provides us an in-depth understanding of government stakeholder-unique requirements. With technology convergence and solution integration, experience matters to deliver business continuity during transition. Whether transitioning like for like services or executing a transformation, a solid transition approach focused on planning and risk management delivers timely transition, which minimizes agency expense. AT&T's transition experience extends beyond the public sector with retail and enterprise business customers. We manage transition every day and will apply that knowledge to assist customer agencies in simplifying the complexity of transition. Furthermore, transition is simplified with a full-service provider that owns the infrastructure on which most EIS services will reside and has the strategic services to overlay on agency networks to provide mission critical benefits. AT&T professionals, using risk management-focused planning tools, can greatly assist agencies in delivering a smooth transition. AT&T is the provider that can transition and deliver low-risk, high-speed transitions locally and globally.

Process: While each transition is unique, there are fundamental and standardized activities that must be performed to decrease the complexity of each one. As depicted in **Figure A-4-1**, the first and most important step is to understand the current state and the desired end state, which is accomplished during planning. During preparation, based on customer input, AT&T jointly creates a Project Plan based on the awarded Task Order (TO) solution. Close collaboration with the agency enables clear and effective tracking



Figure A-4-1. Transition Project Management Process. *Planning and Preparation are key to a successful Implementation.*

of progress until the transition is complete. Lastly comes implementation throughout the process — AT&T provides management and oversight, as does GSA as the EIS contract holder.

Procedures: Based on the degree of complexity and solution details, we determine the right transition model and resources to best meet the implementation requirements. In effect, AT&T right sizes the transition approach and support provided. Those varying configurations of support fall into three primary categories:

1. **Like for Like:** Move the same service from one contract to another (behind the scenes, a record update of the same inventory and the technical requirements).
2. **Upgrade:** Agency adoption of new technology or a refresh of existing solutions.
3. **New Business:** Working with a new agency and incumbent to deliver service via EIS.

Procedures across the transition project management process support the development and execution of the transition plan. **Figure A-4-2** highlights examples of procedures throughout the process.

Tools: Each of the three transition approach scenarios are affected by the volume of components (e.g., circuits, devices or users) and the degree of technical complexity associated with the implementation. Our CSO coordinates the appropriate resources to support transitions throughout the EIS life cycle. These could include Global Project Managers (GPM), subject matters specialists such as in engineering or security, or other AT&T professionals, suppliers or small businesses to extend footprint or capabilities. Each of the groups involved use tools, such as those in **Figure A-4-3**, chosen or designed to support the detail required to properly execute transition.



Figure A-4-2. Transition Project Management Procedures.

Procedures are designed and applied to effectively manage risk.



Figure A-4-3. Transition Project Management Tools.

Effective tools support efficient transitions.

Summary: When an effective transition management approach is fully enabled by a strong foundation of processes, procedures, and tools, GSA and agencies will experience timely, low-risk transitions. AT&T has the depth and breadth of experience, corporate resources, and specialists to enable successful transition of all agencies moving to EIS. The following sub-sections will further address our compliant support for specific requirements stated in RFP Section G.9.4(4).

A-4.1 Transition Project Management [L.30.2.1(4)(a); G.9.4(4)(a)]

The AT&T approach for transition project management from a Networx contract or a GSA Local Services Agreement (LSA) to the EIS contract, and the related responsibilities of GSA and the agencies are shown in detail in **Figure A-4.1-1**. AT&T participates in discussions with GSA and each agency to conduct transition planning and implementation that are consistent with GSA's Transition Strategy and Management Plan (TSMP).

The overarching goal is to individualize the transition support and assistance using an agency-specific TO project plan so the transition is as agile as possible and meets agencies varying requirements. This approach is continually updated to incorporate lessons learned and technology changes when appropriate. We also meet all EIS requirements and provide customers who will be transitioning from Networx to EIS highly secure access to critical BSS applications for ordering, billing, and inventory through the AT&T Business Center portal (**Figure A-4.1-2**) with a single sign-on. As an added convenience for agencies, we have included access to Networx applications within this same single sign-on, so agencies transitioning from Networx to EIS have simplified access to the tools they use to manage their services.



Figure A-4.1-1. Example of Agency-Specific Transition.

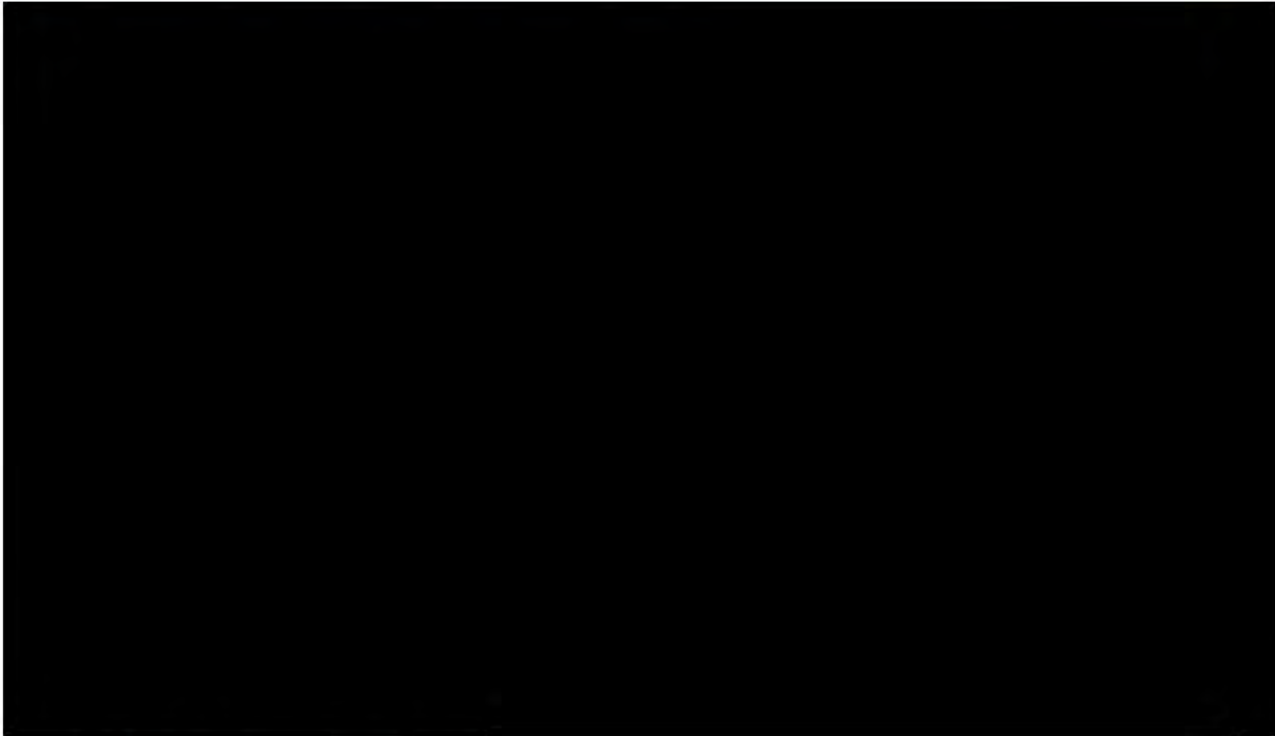


Figure A-4.1-2. Business Center Portal.



Table A-4.1-1.

Table A-4.1-1. AT&T Transition Project Management Features and Benefits.

Approach/Feature	GSA and Agency/Stakeholder Benefits
Conformance with GSA Strategy for Transition Success	- The AT&T transition approach supports GSA success factors which enables conformance with GSA priorities and continuity with agency guidelines - Details are provided in Table A.4.1-2
Hands-on experience utilizing disciplined Transition Approach on agency specific implementations for 48 agencies and 215 sub-agencies	- Agency enjoys a right fit/right time approach that is scalable to each agency. Successful examples include: - Army Recruiting Command: 1728 Recruiting offices transitioned from IPS to NB-IPVPN with inside wiring - AT&T migrated a large retail customer with 18,500 locations of Frame Relay service to Ethernet over AT&T VPN over a 2 ½ year period - Agency benefits from the services of a contractor who has transitioned standard as well as extremely sensitive environments - Transition methodology is based on PMBOK and ITIL foundations - Transition POCs have the reach back into the broader AT&T subject matter specialists to deliver the plan
Global capabilities for a broad set of services and total solutions	- Agency services are supported by 7x24 centers which maintain and monitor AT&T's managed services. An additional two dozen centers support domestic US transport services in order to provide support to infrastructure services offered - To improve operational performance, lessons learned are applied across all functions and based on feedback from all AT&T customers (retail, public, commercial)

Approach/Feature	GSA and Agency/Stakeholder Benefits
	- Over 675 project managers located in over 17 countries are available to support agency infrastructure deployments scope and GSA timeframe 62% of customer service is U.S. based. Breadth and depth commitment of support extends beyond the U.S.
AT&T Global Project Manager Center of Excellence	- Experience of PMI certified project managers enable parallel agency transitions to confidently meet the three-year GSA transition timeframe - GSA/agencies receive the versatility of acquiring expertise with technical subject matter specialists - Global Project Manager (GPM) Center of Excellence, has successfully completed over 4606 projects in 2014 of which 312 were global and approximately 2400 projects are in flight at any one time
Risk Management Plan based on actual not perceived risks	- AT&T's functional and systems knowledge includes feedback and maturation of our risk mitigation approach that is gained from major program transitions in both Federal and Commercial contracts - Includes mitigations strategies derived from lessons learned from both transition "on" and transition "off" experiences - Risks mitigated evidenced in GPM on time project performance: (90% in 2015)

Table A-4.1-2 illustrates that our transition approach is consistent with GSA's transition strategy approach discussed at the EIS industry day in May 2015. AT&T understands the importance of GSA's approach, and has a compliant and compatible framework in support of this plan. This in-depth understanding leads to timely, responsive, and successful transitions.

Table A-4.1-2. AT&T's Transition Activities. *AT&T's Transition approach supports GSA's Transition Strategy for EIS Transition Success.*

GSAs Transition Strategy Approach	
AT&T Transition Activity	Description/Understanding
Pre-Transition/ Pre-Transition Consulting	- Involve key agency functions including agency senior executive "sponsor", transition manager, and lead contracting liaison - Review and validate customer provided inventory prior to transition - Support AHC set up to drive accurate ordering, notices, inventory, & billing - Apply concept of "right size" to tailor transition approach based on agency need - Discuss potential solutions and tradeoffs to upgrade to Internet Protocol (IP) from Time Division Multiplexing (TDM) post-transition versus as part of initial transition to EIS - Use data analytics and trending to offer the customer the optimal solution configuration to meet ever demanding government mission responsibilities
Develop Risk Register	Identify and document known risks and related mitigation strategies. Include: - Risks encountered in similar transition efforts - Agency-specific risks — calendar-related moratoriums, large numbers of remote sites, the need for significant hardware upgrades, agency technology initiatives, and new mandates
Agency Transition Plans	EIS contract-wide planning and implementation: - Basing overall NS2020 transition strategy based on a phased, orderly approach - Working together with GSA to set sequence and pace to even workload on agencies and contractors and make progress early - Inventory analysis, collection and validation of the services is a key step agency-specific planning and implementation conducted by GSA - Assist agencies and GSA as requested to develop agency-specific transition plan

GSAs Transition Strategy Approach	
AT&T Transition Activity	Description/Understanding
	- Deliver agencies' transition plans to GSA and OMB before EIS award (summer 2016) - Allow agencies to transition as their needs require, and at the same time, make new technologies and better cost structures available to agencies when they need them
Agency-Specific Planning	One of the major opportunities for improvement in transition learned from Networkx and regional contracts is more agency commitment during the initiation and planning phases. Customer dependencies include: - GSA provides tailored consulting assistance to agencies for fair opportunity decisions and ordering - Agencies develop requirements based on their unique needs and send the requirements to contractors to bid - Early and effective support is especially important for TO requests which may contain EIS Task Order Unique CLINs (TUC) that are Agency specific - GSA validates inventories continuously to align with EIS Transition timeframe as neither Networkx nor LSAs are static - GSA collaboration to create planning template that assists agencies in preparing for contract transition events
Training (See EIS training plan in Section 2.1.1.7 of our proposal for details)	Training for the agency customers will maximize their experience with the EIS contract by focusing on the product offers and the AT&T BSS platform tools that will support customer business operations. Training is provided by the AT&T EIS training team and include: - Train the government trainer - Government executive overview training designed to cover the fundamentals - CO/COR focused on tools and processes to run the EIS contract with a focus on ordering, billing and maintenance - Transition classes for CO/COR and Network Operations Center (NOC) personnel to understand resources to provide a smooth transition - Supplemental training: agency may request additional (specialized) training in a TO
Kick-Off with identified Agency Transition Point of Contact (POC)	- Approach is a standard planning process to allow Agency customers, suppliers, and AT&T to review and agree on all aspects of the transition, including specific timeframes, effect on current agency mission(s), and related risks. As applicable, identify new mission objectives and technologies that may have been introduced - Checklist of common items: post-award planning, and standardized set of planning deliverables. This process is completed before any transition orders are issued
Service Transition/Reporting	To enable transparent and meaningful reporting, in working with each agency including: - Establish stakeholder communications standards to provide transparency for reporting progress on all aspects of the contract transition - Confirm metrics convey the relative complexity, level of effort and transition - Accommodate the breadth of services and the broad range of agency missions, technical capabilities, geographic scopes, and operating environments - Provide periodic status updates using common dashboard and common definitions - Measure overall program transition progress towards completion based on value or criticality of what has been transitioned (e.g., percentage of Networkx/regional revenue discontinued, or percentage of core capabilities transitioned)

A-4.1.1 Billing, Service Ordering, Trouble Reporting, and Customer Service Processes That Are Unique for Transitioning onto EIS and off EIS [L.30.2.1(4)(a); G.9.4(4)(a)]

AT&T applies established standards and a disciplined approach to all EIS transitions. Agency-specific Task Order Project Plans (TOPPs) detail unique transition requirements. **Table A-4.1.1-1** summarizes our approach to each functional process.

Table A-4.1.1-1. Approach to Functional Processes. AT&T has in-place transition functional processes to complete timely transition for each agency.

Functions	Summary Approach
Billing	- Pre-transition consulting such as: - Desired Billing Features —Direct Billing, Bill Media Format, etc. - AHC set up to confirm accurate inventory and billing - If known Billing or Inventory problem, develop steps to mitigate prior to Transition - First bill reviews will be conducted with the customer to confirm billing accuracy
Service Ordering	Service Ordering approach based on transition type: 'Like for like' from existing AT&T contract to EIS will be handled as an EIS administrative order - Transformation of existing AT&T service to new technology on EIS will benefit customer mission and be supported with a Transition project plan to deliver service continuity - Transition of services from an incumbent provider to AT&T may include a TOPP to confirm coordination between service providers - If EIS TUCs are in scope, review component composition and scope of work to confirm all individual orders are properly sequenced and managed
Trouble Reporting	- After a successful transition, services will move to EIS lifecycle phase - Agency COs to be trained and given access to web-based tools to manage and monitor service - Maps and maintenance application will continue to allow customer to self-serve and view current ticket status, as it does today on existing contracts - Newer product-specific portals (e.g., cloud products) allow customer to dynamically interact via live chat function for support questions on their service
Customer Service	- As noted in Section 1.1.4, agency assigned client executives are the primary advocate for customers and determine best solution for agency transition - Transition project manager take hand off from assigned client executives and work directly with agency representatives to establish transition plan milestones, schedule, and confirm available resources - Problem identification and resolution (including trouble reporting) are reviewed with the agency to implement lessons learned and to mitigate future reoccurrence - Specific training is provided to facilitate customer understanding of PM tools and processes - If EIS TUC CLINs are in scope, review component composition and scope of work to identify if standard component or non-standard reporting is required either during implementation or as part of life cycle

Transition On: AT&T works closely with GSA and agencies to conduct a phased approach, which will mitigate schedule risk and support completion of all required transitions not later than three years after contract award.

Upgrading or replacing active services from another contract to EIS does not have to be specifically marked as Transition. However, they will follow the same planning and project management approach to minimize impact on the ordering agency's operations when cutting over to the replacement service. Agency-unique requirements can be accommodated within the EIS TO structure. Experienced AT&T team members support agencies to execute transition until we have achieved a successful steady state.

Transition Off: As part of the Transition Off planning with GSA, in support of EIS contract expiration, AT&T will provide advice on strategies to minimize transition time and risk. With knowledge of agency-specific services and broader technology futures

and solutions, AT&T can further support GSA with product or solution-specific strategies to improve transition timeliness. RFP Section C.3.3.2 requests discussion of support for PIC/LPIC changes. Within this proposal, AT&T is bidding Internet Protocol (IP) Voice Service for which no PIC/LPIC nor Letter of Authorization is required to support long distance carrier changes. Long distance automatically defaults to the carrier providing the voice over IP access. Examples of service-specific transition off steps are shown in **Table A-4.1.1-2**.

Table A-4.1.1-2. Examples of Transition Off Planning. *AT&T has mature process steps based on extensive project management experience throughout the enterprise that enables us to minimize transition time.*

Example 1: Dedicated Access & AT&T Roles	▪ Receive disconnect access service order including circuit identification, speed, and type. ▪ Review inventory for inaccuracies and communicate any discrepancies in inventory against AT&T and Local Exchange Company (LEC) databases, for accuracy and missing circuit information ▪ Forward discrepancies to the customer agency and assist in resolving issues ▪ Communicate disconnect interval and due date to customer so agency can coordinate with new provider ▪ Initiate disconnect order ▪ Advise agency of completed orders once disconnect complete
Example 2: Premise Based Service & AT&T Roles	▪ Attend kick off call hosted by the customer and/or new provider ▪ Receive disconnect order for Transition Off ▪ Validate inventory and applications supported by premised based unit against AT&T documented Technical Provisioning Document (TPD) ▪ Communicate disconnect interval so agency can coordinate with new provider ▪ Initiate disconnect orders ▪ Cutover of routes/traffic Transition Off to new provider in coordinated manner ▪ Continue with service disconnect process once service migrated and confirmed working ▪ Service-Related Equipment (SRE) is boxed and shipped back to AT&T facility to be wiped and disposed within 45-day retrieval interval ▪ Advise agency of completed orders

In accordance with RFP Section C.3.3.3, AT&T will provide the government the following transition inventory, monthly validations, and summaries:

- For the final five years of the contract, AT&T will conduct periodic validations (approximately once every six months) of its transition inventory with GSA and reconcile any discrepancies.
- If GSA exercises all the contract options for the final three years of the contract, we will conduct monthly validations with GSA
- At the GSA CO's request, AT&T will deliver an inventory summary of all services active, that is, in service, whether in use or not, at the time of the request, by Agency Bureau (AB) code, service, quantity, and location

- At the OCO's request, we will deliver an inventory summary of all the agency's services active at the time of the request

If GSA exercises all the contract options, for the final three years of the contract, AT&T will deliver weekly reports of services disconnected and active services based upon the transition inventory. During that same three-year period we will deliver a monthly Transition Status Report that includes:

- Data file of invoiced amount by AB code for the most recently completed billing period
- Discussion of transition issues reported by agency customers or AT&T either during the reporting period or unresolved since the last report, corrective action, and status
- Risk analysis and response plan

A-4.1.2 How AT&T will Expedite Transition When AT&T Is Also the Incumbent Service Provider [L.30.2.1(4)(a); G.9.4(4)(a)]

The most effective way to expedite transition, as shown in **Table A-4.1.2-1**, is to work closely with the customer throughout the transition process, especially during the planning phases. Effective communication and planning are critical. The AT&T disciplined transition approach allows a high-quality low-risk plan to meet mutually agreeable timelines that support customer missions.

Table A-4.1.2-1. Expediting Transition as the Incumbent. *AT&T focuses on the planning process to effectively work with the customer.*

Transition Type	Sample Ways to Expedite Transition. Details Vary by Solution.
Like for Like	- Planning: Validate physical and billing inventory prior to transition. - Post transition, confirm accurate inventory
Upgrade	- Planning: Validate physical and billing inventory prior to transition. - Jointly test configuration or design prior to upgrade. - In some cases, it may be more beneficial to transition like for like initially, then subsequently transform communications solution in phases
New	- If part of TO, replicate configuration or design in lab prior to deployment to minimize risks and reduce implementation time. - Lessons learned applied from prior customers service implementations

If expedited CLINs are included on a transition order, we review support on a case-by-case basis following a standard methodology so that a comprehensive approach is developed. AT&T has resources whose experience allows maximum flexibility to respond to expedited orders and adapt to multiple, complex priorities and agency requirements.

In addition, if a mapping between EIS and Networkx CLINs is available, it could be used to expedite processing of orders to move an existing Networkx customer to EIS with like for like services.

A-4.1.3 AT&T Will Coordinate with Other Incumbent Providers to Ensure a Smooth, Successful, and Timely Transition [L.30.2.1(4)(a); G.9.4(4)(a)]

AT&T provides smooth, successful, and timely transitions following standard AT&T transition processes as defined within our transition management approach. AT&T builds upon lessons learned from existing Transition Management Plans (TMPs) for other contracts including Networkx and will deliver consistent transition services for the EIS statement of work.

AT&T has established relationships with existing incumbent service providers, access providers, suppliers, vendors, and other agency providers. When working with incumbents, we implement industry standard turnover processes, practices, standards, schedules, and a risk management plan. We communicate requirements and work with the incumbent as part of planning process with the agency so the incumbent can provide input to AT&T and the CO/COR/GSA. All activities requiring coordination with other incumbent providers are managed by the assigned transition project manager, assigned to work a particular transition, who works with existing provider(s) to deliver a smooth transition with limited, if any, downtime.

A-4.1.4 Identification and Assessment of the Major Transition Risks and the Proposed Response to Each [L.30.2.1(4)(a); G.9.4(4)(a)]

Our experience on managing and mitigating transition risks is essential to help GSA and agencies migrate successfully to EIS. Transitions can be complex and difficult when industry-leading practices are not agreed-upon without formal process adherence. American Council for Technology and the Industry Advisory Council (ACT-IAC) established a committee focused on transition to incorporate industry guidance and lessons learned after the Networkx transition GAO audit. AT&T actively participated with industry and the GSA EIS Program team prior to Final EIS RFP release.

Figure A-4.1.4-1 identifies principal transition risks and our mitigation plan to address these risk areas. Additional risk management information is provided in **Section A-8**, Risk Management Plan.

AT&T understands that transitioning inventory requires diligence to provide accuracy, accountability, and integrity within our EIS inventory management system. Several critical steps include: (1) work with GSA and agency POCs to create inventories and a transition plan, (2) review agency provided Transition Plan as part of the planning process, (3) validate customer provided inventories from the incumbent, and (4) assist OCOs with placing task and service orders to confirm accuracy, completeness, and timeliness. This helps minimize complexity, risks, and delays in transitioning.

Risk to Transition	Probability of Risk	Impact of Risk	AT&T Approach
Inaccurate inventory information provided by GSA, agencies and incumbents.			Use all available data sources to build the transition inventory database. Begin as early as possible. Use site visits as needed. Communication and tracking of detailed information requirements, correlation and validation of known data elements, persistent tracking and quality reviews.
Local government contacts unsure of their role and responsibilities for support.			GSA and transition team create site cutover form explaining transition, site visits and local government contact responsibilities. Establish backup local government contact at each site. Obtain local government contact agreement of their responsibilities.
LEC circuit deliveries do not meet transition schedules.			Use extended order intervals to reduce the risk of late deliveries, with increased throughput to meet schedules. Negotiate for LEC project management and schedule prior to order issuance.
Transition Scope and Schedule changes.			Institute change control process, team reviews impact of the change.
Resource availability to meet anticipated workload.			Prepare preliminary schedules based on order volume and throughput. Perform feasibility study and communicate staffing needs of CPO, CSO and support needs of contractor and supplier organizations based on the work.
AT&T Circuit Facility Availability (CFA).			Obtain site list prior to order issuance and utilize the large project planning process to perform feasibility and capacity verification. Adjust schedules to allow for site transition based on facility availability.
Agency delays in supplying necessary ordering information.			Create transition schedule with milestone tasks detailing impact of delays in information receipt. Include customer delay/response in escalation and resolution plans.
Under EIS, each agency is assuming a new role in supporting TO processing between different contractors.			Use AT&T standardized contract modification template which was utilized successfully with GSA to facilitate agency TO development and processing.
Implementation of new technologies and technology replacements which becomes more critical with ever shortening technology life cycles.			Work with agencies to jointly create transition risk plans and contingency plans by using corporate subject matter specialists and program/project managers. As appropriate, jointly develop plan to include test in labs then 'soak' new technologies on limited scale prior to full deployment.
Risk Level:  = High  = Medium  = Low			

Figure A-4.1.4-1. Principle Transition Risks Register. Our transition risk mitigation strategies are developed from hands-on experience performing transitions for over 180 agencies and experience from commercial customers.

A-4.2 Agency Solicitations [L.30.2.1(4)(b); G.9.4(4)(b)]

As shown in **Table A-4.2-1**, to facilitate quotations and proposals, AT&T has a team of client executives dedicated to working with specific agencies and customers to help them identify and select new or enhanced services to replace services on existing contracts. These client executives have long term, cohesive relationships with their agency customers, and stay connected to them as Transition project managers take over the actual delivery of services ordered.

Table A-4.2-1. Quotations and Proposals. *AT&T customer interaction is focused on providing the right solution for each agency.*

#	AT&T Customer Interaction
1	AT&T sales client Executives consult with the appropriate agency personnel during market research, quotation or proposal and requirement development to determine the most effective agency solution on EIS.
2	AT&T sales client executives use full AT&T capabilities and breadth of service offer to respond to agency RFQs and RFPs with solutions that best address the requirements of the agency to replace its existing services with solutions of equal or better levels of performance, ease of use, and competitive pricing.
3	Certain phases may necessitate AT&T personnel being dedicated to focus on those phases and interact with dedicated government personnel; TOs can accommodate agency requirements for AT&T to identify its personnel by name as part of the agency-specific EIS TOPP.

A-4.2.1 Approach to Assisting Agencies with Selecting New or Enhanced Services to Replace Services on Expiring Contracts [L.30.2.1(4)(b); G.9.4(4)(b)]

Transition planning is a natural opportunity to review pricing and functionality of services and determine if additional capability through the selection of enhanced features can produce expense reduction, consolidation or transformative experiences for the agency users. AT&T client executive teams have agency-specific focus, knowledge, and expertise as well as unified relationships with their supportive agency staff. These client executive teams will be our primary points of contact on the identification, evaluation, and selection of new or enhanced services to replace existing services.

AT&T will provide the GSA and or agency personnel training and guidance on service availability. In addition, AT&T will provide a solution's value to refine the expense of the transition and or schedule improvements. Inherent in these discussions are the objectives of the agency mission, resources required, and the associated expenses that influence transition approach. These discussions are conducted by our dedicated client executive teams, all of whom have specific expertise supporting a particular agency.

Table A-4.2.1-1 below lists some of the actions performed to assist agencies.

Table A-4.2.1-1. Approach to Assisting Agencies. *AT&T expertise provides a detailed understanding and clarity to agencies requiring new or enhanced services.*

Approach to Assisting Agencies
- Work with GSA and agencies on new solutions to retire aging TDM technology and speed adoption of IP-based technologies - Provide guidance to agency personnel how to order service in the most effective way - Deliver comprehensive solutions that address mission critical needs - Introduce forward-looking service strategies including Software Defined Networking (SDN), NetBond, Mobile Applications, and Cloud - Promotes a "network on demand" and "digital first" platform strategy to allow flexibility for agency operations

A-4.2.2 Incentives to Expedite Transition [L.30.2.1(4)(b); G.9.4(4)(b)]

AT&T will work with GSA and the agencies to help plan and execute a timely transition to EIS. AT&T uses a variety of customer-focused support initiatives to meet the three-year transition timeline objective and provide business continuity of agency operations. AT&T support includes:

- Development on GSA's TSMP as part of ACT-IAC
- Prior to award, present agencies with cost and operational benefits of different technologies and elements of successful transition so they are prepared
- Team with named GSA resources assigned to support agencies to validate agency-created Transition Plan and agency-provided inventories
- Existing agency client executive and customer service teams will work with the agency on an individual basis to make sure a quality transition is performed from existing contract to EIS.
- Scale to offer value pricing on broad range of products and locations (CBSA) to provide a total solution satisfying agency needs
- In addition, if a mapping between EIS and Networx CLINs is available, it could be used to expedite processing of orders to move an existing Networx customer to EIS with like for like services.

A-4.3 Customer Support During Transition [L.30.2.1(4)(c); G.9.4(4)(c)]

The AT&T comprehensive customer support model uses company-wide resources to facilitate customer EIS transition and include:

- **Advocate:** Existing client executives are the focal point for assisting agencies with service requirements analysis for development of the best customer solution
- **Execute:** The AT&T Transition Manager directs assigned resources to support overall customer implementation. In addition to agency specific life cycle service managers, AT&T uses global project managers to facilitate parallel transition implementations.
- **Promote:** AT&T functional subject matter specialists (e.g., security, professional services, etc.) are available to deliver quality implementations and business continuity.

A-4.3.1 Describe and Provide An Outline for Any Transition Handbooks or Guides that AT&T Will Make Available to Customers [L.30.2.1(4)(c); G.9.4(4)(c)]

Within each of our transition handbooks and guides provided, we include a standard, base set of information that can be tailored to the agency to efficiently coordinate transition. That includes an outline containing roles and responsibilities, contact information of all transition project team members, Project Staffing Plan, Installation Planning and Schedule, Testing Schedule, Proposed Migration Plan, Pre-installation Planning, Test and Acceptance Plans, Risk Management Methodology, etc. Agencies may receive an overall plan with multiple product sub plans as dictated by TO award details.

A-4.3.2 Provide Target Date for Publication [L.30.2.1(4)(c); G.9.4(4)(c)]

AT&T intends to publish outlines for handbooks and guides within 30 days after EIS contract award. Agencies can receive the applicable handbook/guide upon individual TO award.

A-4.4 Interconnection Plan [L.30.2.1(4)(d); G.9.4(4)(d)]

When working through network providers for access services, AT&T provisions with a primary focus on maintaining continuity and quality of service throughout the cutover.

AT&T's plan consists of quality checks prior to any transition of access services.

A-4.4.1 Description of Interconnection Arrangements Between the Incumbent Contractor's Network and the EIS Networks during the Transition, Including the Interconnection Arrangements with the Local Exchange Network, the IXC's, and Government Private Networks [L.30.2.1(4)(d); G.9.4(4)(d)]

During the planning process, AT&T works with the agency to develop strategies for interconnectivity between the AT&T network and the incumbent provider's network for the purpose of transition. Planning is based upon a specific solution to provide continuity of service for all sites. AT&T will assign a transition manager who works closely with the customer agency to review the inventory received and verify accuracy of the data. Additional discussion of our inventory process can be found in **Section 1.1.6**.

Interconnection transitions are easily facilitated by our relationships and interconnection arrangements with all carriers, which is how we hand off traffic between carriers. AT&T has carrier relation managers who own carrier performance for access provisioning and

maintenance with other major carriers (e.g., Verizon, FiberLight, etc.) and can facilitate incremental support as needed. These arrangements can be extended or modified to include arrangements for local exchanges, IXC's, and government private networks. Multiple interconnect plans can be designed and validated based on specific transition types, agency requirements, configuration, and solution.

A-4.4.2 Description of Any Interconnections with Other Service Providers, Including Other Operating Units Within AT&T Such As Wholesale Services, Known or Expected to be Required to Transition Services [L.30.2.1(4)(d); G.9.4(4)(d)]

The planning and execution approach in **Section A-4.4.1** applies to all interconnection plans regardless if it is another service provider or operating unit within AT&T.

A-4.4.3 Potential Impact to Customers' Operations [L.30.2.1(4)(d); G.9.4(4)(d)]

The transition risk plan includes detailed steps to minimize potential disruptions.

Representative examples, not fully inclusive, include those shown in **Table A-4.4.3-1**.

Table A-4.4.3-1. Example Steps to Mitigate Possible Impact to Customers Operations. *AT&T has established process steps to address critical areas of impact that may affect customer service.*

Example 1: Dedicated Access	▪ Risk: Dedicated access links are not available due to poor advanced capacity assessment or are not timely due to delays in the ordering and provisioning process. ▪ Mitigation: Obtain inventory of local and Inter Exchange Company (IXC) circuit information including circuit identification, speed, and type: – Review inventory for inaccuracies and forward to the assigned project implementation team to scrub the inventory against AT&T and LEC databases, for accuracy and missing circuit information – Perform address validation – Forward discrepancies to the customer agency and assist in resolving issues – Load circuit information in AT&T provisioning databases – Test and validate service working – Advise agency of completed orders, resolve rejected orders
Example 2: Establishment of Gateways	▪ Risk: Gateways, also called protocol converters, can operate at any network layer. The activities of a gateway are more complex than that of a router or switch, so the planning and preparation are critical to minimize any impacts to agency operations. ▪ Mitigation: A typical transition to Internet Protocol (IP)-Virtual Private Network (VPN) includes the following high-level steps: – The connection of the gateway sites for routing between transitioned and non-transitioned sites. This includes: ○ The selection of the gateway site(s) ○ The connection of the gateway site(s) to the VPN ○ The advertisement of routes needed for transition from gateway sites into the VPN – The transition of agency sites to the VPN includes: ○ The connection of the site to the VPN and pre-cutover validation of connectivity through the VPN ○ The cutover of site traffic to the VPN ○ Confirmation of operational traffic continuity with customer ○ Agency advised of completed orders

A-4.5 Transition Contingency Plan [L.30.2.1(4)(e); G.9.4(4)(e)]

During the detailed planning and preparation phases of transition management, AT&T identifies and documents contingency procedures for each service ordered. Technical details vary depending on agency solution and configuration. We eliminate downtime by designing a transition approach that allows a smooth cutover and allows for response to unforeseen difficulties and fall back by location using gateways, and custom routing. AT&T validates and confirms any fallback procedures with the incumbent provider, in accordance with the contingency plan. Contingency procedures are applicable to all stages of transition and contain specific tasks, activities, responsible parties, and timeframes necessary to confirm that service is restored to the original status. No cut over is executed without a detail fall back strategy that can be executed within the approved maintenance window. The roles and responsibilities of the participants are shown in **Table A-4.5-1**.

Table A-4.5-1. Transition Contingency Roles and Responsibilities. *AT&T coordinates with the agency and incumbent service providers to properly define each stakeholder's activities and roles during contingency operations.*

AT&T	Draft specific contingency/fallback procedures based upon: the specifics of the technology to be implemented, the design of the solution, the detailed transition plan and the specific customer requirements of the contingency/fallback strategy. AT&T will have a lead role.
Agency	Provide a primary point of contact that will serve as a liaison with agency engineers and agency decision makers. It will also be the responsibility of the agency to confirm that the incumbent service provider is present during contingency/fallback planning activities. The agency will have the following roles: technical support, customer decision maker, and liaison with incumbent.
Incumbent	Be present during the contingency/fallback planning and to sign-off on agreed upon specific activities. The incumbent role is: technical support and sign-off agreement.

Once completed, contingency procedures are reviewed with the agency and the incumbent for completeness during planning phases. Prior to actual cutover of services, contingency procedures are reviewed again with the incumbent and the agency to adapt to any changes made since procedures were created. Processes to restore service when unforeseen difficulties are encountered in relation to cutovers, no parallel processes, and parallel processes are shown in **Table A-4.5-2**.

Table A-4.5-2. Processes for Contingency/Fall-Back. *In each scenario, AT&T will execute contingency plans to minimize impact to operations when unforeseen difficulties arise.*

Contingency/Fall Back Processes for Unforeseen Difficulties	
Cutovers with System Downtime	If systems downtime is required for cutover activities, AT&T will establish parallel processes and Systems availability (up time) will be scheduled.
No Parallel Processes	- Follow all established escalation and issue resolution paths - Review and confirm that all potential work around scenarios are assessed and ruled out as possible stop-gap solutions - Trigger contingency/fallback:

Contingency/Fall Back Processes for Unforeseen Difficulties	
	– Notify affected parties and need-to-know executive decision makers of fallback – Kick off contingency/fallback activities as per previously agreed upon exit/migration fallback tasks and activities, responsible parties, and timeframes – Incumbent tests and validates incumbent systems – Allow end-user access to incumbent (systems up) ▪ Conduct post-mortem and next steps
Parallel Processes	▪ Make sure all escalation and issue resolution options are fully explored and exhausted ▪ Confirm all potential work around scenarios are discussed and ruled out as possible stop-gap solutions ▪ Trigger contingency/fallback: – Notify affected parties and need-to-know executive decision makers of contingency/fallback – Notify end-users to continue to use incumbent until further notice (only difference from “no parallel processes” fallback procedures) ▪ Conduct post-mortem and next steps

A-4.6 Additional Areas Proposed by AT&T [G.9.4(4)]

Our proposal demonstrated approach to transition of services, which is comprehensively described in **Section A-4.1 – Section A-4.5**.

A-5 Resource Plan [L.30.2.1(5); G.9.4(5)]

GSA will benefit from working with a resourceful and established EIS provider that uses resource management approaches developed in conjunction with GSA over two decades providing communications services to the federal government.

The AT&T Resource Plan for, and approach to managing financial, human, and hardware/software equipment resources applies our two decades' experience working with GSA to deliver communications service to the federal government. The EIS PM will use, and uses today on Networx, documented, repeatable AT&T standard processes to manage finances, personnel, and assets. So while GSA incurs no direct labor cost to manage the contract, repeatable processes still benefit the government by having in place a structure tooled to deliver service efficiently to EIS subscribers.

A-5.1 Financial Resources [L.30.2.1(5)(a); G.9.4(5)(a)]

Budget: The EIS CSO monitors and reports on finances to GSA as prescribed in the RFP Section F.2.1, and according to requirements contained in RFP Section G. The Monthly Financial Status Report (Deliverable #80) captures spend against contract ceiling limits by agency, by TO, by EIS service area, and by direct billing TO. The AT&T automated biller functionality tracks system and service usage on each account. In addition to producing invoices, the biller also generates contract-specific reporting

artifacts tailored to meet EIS requirements for delivery to the government. These reports transmit to the EIS CSO via the BSS. CSO compiles financial status reports and forwards them to contracts for review, validation, and submittal to GSA as an official deliverable. The process is automated, with quality spot checks performed at by the CSO and by contracts. The CSO manages EIS against internal baseline budgets to deliver the proper level of service to the government. Those budgets are internal AT&T controls, as CSO is not direct billed to the government. Individual TOs might require budgets. In those cases, budgets are established with individual agencies and managed locally.

Tracking Costs: AT&T uses standardized financial workbooks hosted on our highly secure internal BSS, integrated with project management processes, to track expenses. Through the BSS, the CSO accesses TO-level finances, collect service level data, financial data, can monitor performance at individual agencies, and generate monthly financial status reporting deliverables. To the extent professional services or direct labor is required as a component of a particular TO, the TO lead (i.e., client executive) uses standardized and repeatable AT&T expense and TO management approach, depicted here in **Figure A-5.1-1**.

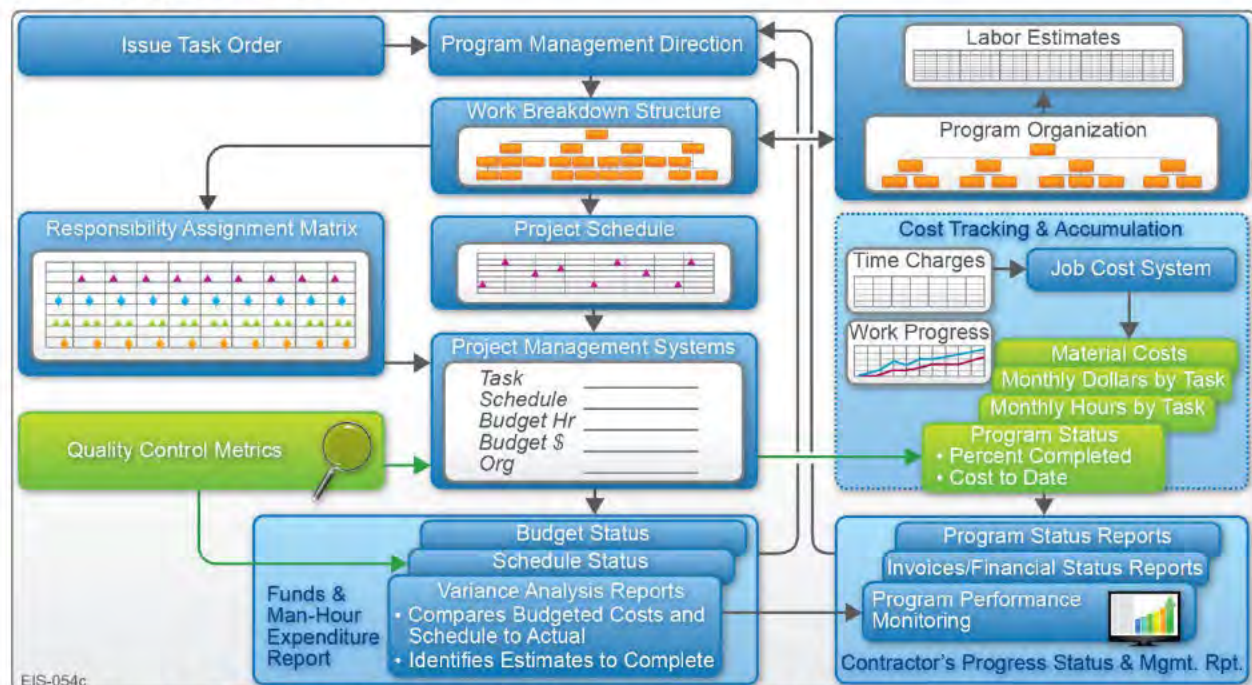


Figure A-5.1-1. Managing Financial Resources. Our accurate estimating and tracking procedures provide GSA and agency customers with complete on-line understand of financial status.

Status reports include billed charges for the reporting period for direct billing accounts. The CSO keeps the GSA COR and COTR informed of program performance via defined reporting according to EIS RFP requirements.

Controlling Costs: AT&T is a full-service provider. For EIS, GSA and government agencies will tie into an existing network — not one that needs to be stood up upon award — but an existing network into which AT&T invests \$63 million per day enhancing and improving. Our scope and spend allows us the ability to negotiate with suppliers for the superior prices, and to facilitate appropriately pricing services for each market. Cost control for AT&T products, services and infrastructure is mainly a corporate function, with the benefits to GSA and the federal government manifested in the Price Volume of this proposal. AT&T monitors and costs through three primary methods: (1) Competition among regional carriers and providers exerts downward pressure on price; (2) We continually monitor competitor prices to be sure we are competitive regionally and across all our services; (3) AT&T has invested almost \$23B each year (\$63 million/day) to enhance its network and develop newer, cost effective services. Investments drive down non-recurring and recurring charges. This mass investment benefits GSA in the form of competitive prices and improved reliability to service the federal government. These also benefit the government at the Task Order level.

A-5.2 Human Resources [L.30.2.1(5)(b); G.9.4(5)(b)]

AT&T human resource managers employ repeatable processes to identify, retain, and deploy highly skilled professionals for government customers with maximum efficiency. AT&T employs multiple approaches to meet program, project, and development needs, for EIS, and company-wide.

Identifying Qualified Personnel: AT&T is a top-25 global company, so hiring and retention of talent is a strategic initiative. AT&T recruiters work continually to identify individuals with strategic skillsets to provide available, qualified staff as needed to meet government requirements. Our hiring process (**Figure A-5.2-1**) has proven responsive and successful on multiple federal engagements including Networkx.



Figure A-5.2-1. AT&T Hiring Process. *The AT&T established hiring process attracts high quality personnel to support EIS.*

Our recruiters use traditional and cutting-edge recruiting tools such as social media search efforts to find qualified candidates. Internally, AT&T provides incentives to employees for identifying and recruiting talent. Veterans comprise a critical pool of skilled potential workers. In 2013, AT&T committed to hire 10,000 veterans by 2018. At this writing, we have hired more than 7,000. In addition, AT&T hosts over 600 college interns each summer and attracts experienced industry professionals in a diverse workforce with a broad perspective. When a staff need is identified, the PM opens a requisition for a new position, which in turn engages the AT&T recruiting staff. Recruiters assess candidates and to confirm each meets education, certification, technical skills, citizenship, and security clearances required. The recruiter then forwards acceptable candidates to hiring managers for interview and hiring decisions.

Retaining Qualified Personnel: Table A-5.2-1 highlights AT&Ts training, compensation, and credentialing efforts that increase skills and improve retention.

Table A-5.2-1. AT&T Comprehensive Employee Retention Programs. *GSA and EIS subscribing agencies receive world-class support from our experienced and highly trained personnel.*

Retention Programs	AT&T Program Approaches
Competitive Compensation Plans	AT&T maintains continuous participation in compensation surveys to verify workforce salaries are competitive and consistent with the market for specific regions
Routine Reviews and Opportunities for Advancement	Each employee has an Individual Development Plan (IDP) to set a strategy for keeping employee skills current and facilitating their professional growth. Getting the right people on the team, providing direction, giving feedback, and helping them grow and develop results in high-performing teams anywhere within the company.
Employee Net Promoter Score (eNPS)	Open communication gives everyone equal participation in the success of our business. AT&T administers an employee engagement survey three times a year to facilitate continuous feedback to leadership.
Forums	AT&T promotes involvement in professional, government and industry forums encouraging the exchange of ideas, professional recognition, and growth.

Retention Programs	AT&T Program Approaches
Employee Resource Groups (ERG)	AT&T has twelve ERGs that are open to all employees reflecting the diversity of company employees. For over 45 years, ERGs support the company's commitment to diversity and inclusion through their efforts in the workplace, marketplace and the community. Over 94,000 employees belong to ERGs and volunteered 302,000 hours in 2014.
Leading with Distinction	Our world-class leadership and strategic alignment initiative and cornerstone development program empower all managers to lead their organizations in alignment with our three-year business plan to accelerate growth and to drive an organizational culture committed to innovation.
Nanodegrees	As network and business transformation gains momentum, the demand for new skills continues to accelerate. AT&T has partnered with Udacity on self-paced, fast-track technical credentials called nanodegree programs for high-demand tech jobs.
Tuition Reimbursement	AT&T maintains a generous tuition assistance program to help employees complete degrees that expand their qualifications and capabilities. This encouragement to increase staff credentials and qualifications enhances employee satisfaction and thus retention.
Professional Certifications	AT&T funds employee professional programs, including the PMI certification and technology certification programs including fields of computer science, cyber security, data science and Software Defined Network (SDN).

Effective Use of Skills: As delineated in **Table A-5.2-2**, EIS will employ approaches to deploy staff based on skill, customer need, development, and competitive prices.

Table A-5.2-2. Methodologies for Effective Utilization of Personnel. *Effective deployment of staff enables AT&T to manage expenses efficiently and retains institutional and product expertise.*

AT&T Program Approaches	Benefits
Continuous use of predictive analysis and bottom-up requirements analysis to estimate staffing needs	Reduces service lag by allowing EIS managers to anticipate staffing needs and make assignments early, manage pipeline
Cross-team mobility uses our depth of strategic skill sets and talent residing across AT&T	Provides GSA team members with broader experience base and exposure to multiple methodologies
Using location-based skilled personnel whenever possible to reduce travel costs and increase productive time.	Minimizes charges to GSA and agencies, while providing staff with unique ad-hoc staffing and skill-building opportunities
Employing resources from the same labor mix across agencies for cost savings, continuity, and risk mitigation.	Provides GSA and agencies with resources more rapidly, uses skills from wherever they exist within the company to meet mission needs faster
Fostering productivity with open communications, exchange of ideas, and empowerment to make decisions.	Benefits government through reduced turnover by improving employee morale via access to leaders and internal exchange
Training and mentoring programs to enhance skill sets and productivity.	Reduces turnover by providing an unofficial apprenticeship encouraging staff to learn from more experienced practitioners
Knowledge sharing sponsored by business units and market leads such as Get Smart Forums and local get-togethers for skill building and knowledge sharing across all functions.	Benefits GSA and government by keeping staff skills up-to-date and proactively engaging in formal and informal knowledge exchanges and social activities that expose staff to other parts of the company

A-5.3 Equipment [L.30.2.1(5)(c); G.9.4(5)(c)]

In instances where hardware and software are components of the EIS contract, AT&T is committed to procuring and managing equipment and software assets in accordance

with SCRM security requirements. We are certified under the TL 9000 Quality Management System (QMS) to meet the supply chain quality requirements of the worldwide telecommunications industry.

Managing Hardware and Software Assets: GSA and its EIS subscriber agencies have widely varying hardware, software, and inventory management requirements. AT&T uses the asset management application, which will be adapted for EIS to provide timely and accurate asset status on assets associated with managed services. Coupled with our eProcurement system, AT&T manages the flow of and disposition of equipment through the asset management phases: procurement, life cycle, and retrieval/disposal.

Procurement Phase: Installation technicians and vendors feed procurement data, serial numbers, device identifying data, and location to downstream AT&T databases used to manage assets in the lifecycle and disposal phases.

Life Cycle Phase: AT&T uses hardware (HW) asset location data for break/fix replacement and retrieval purposes. Serial number and asset data are updated when replacement devices are swapped for faulty ones. The AT&T life cycle team monitors vendor performance and will renew EIS maintenance plans and SW licenses as necessary based on asset status (e.g., renewal, upgrades, disconnects). AT&T will produce and provide an Inventory Reconciliation Report to GSA and individual agency CORs to review by the 15th of each month.

Retrieval/Disposal Phase: AT&T maintains a team dedicated to recovery and proper disposal of IT assets. We have dozens of approved vendors nationwide authorized to clean/wipe, shred, destroy, resell, and/or scrap IT hardware, which will be deployed under EIS, located nationwide to service all agencies. AT&T-managed devices can be wiped remotely if connected to the network prior to final disconnect. Alternately, technicians can retrieve EIS hardware from agency sites, wiping devices prior to removal from premises. As a final safeguard, EIS hardware is checked upon arrival at the final disposition location.

AT&T brings to EIS a mature set of resource management processes and capabilities, established and refined over more than twenty years of service to GSA delivering world class communications services to the federal government.

Did You Know?

Our commitment to sustainable asset disposal is written into company policy as Operating Practice No. 123 "Disposition Services Policy and Procedures."

A-6 Quality Control Program [L.30.2.1(6); G.9.4(6)]

GSA and agencies will receive a well-structured and rigorous Quality Control program providing confidence that all EIS services and work are executed to high standards of performance. Quality Management consists of a number of components, as described in **Table A-6-1**.

Table A-6-1. Quality Management Terms.

Quality Management Terms	
Quality Management	
Quality Planning	
Quality Control (QC)	
Quality Assurance (QA)	
Quality Assurance Surveillance Plan (QASP)	

AT&T's EIS Program Manager (PM) and her team continually work to enhance our customer service processes. We will collaboratively inform the GSA

program management and agency Task Order Managers of our current performance, variances with respect to plans and our proposals to address the variances. The EIS Quality Management Program is informed and supported by AT&T's Quality Center of Excellence (COE) and Quality Management System (QMS) (**Table A-6-2**), which provide tools, support, and expertise to enhance our quality management capabilities.

Table A-6-2. AT&T QMS.

AT&T QMS	
Six Sigma	
Management System and Operating Control (MSOC)	
Lean	
Quality by Design	

Table A-6-3 shows how GSA and the agencies benefit from our quality control program.

Table A-6-3. Quality Control Approach and Capabilities. *The quality control program designed for EIS builds upon the successful program for Networx and demonstrates our corporate commitment to continuous improvement.*

Evaluation Factor	Approach	Benefit	Capability

A-6.1 Management Approach for Formulating and Enforcing Work and Quality Standards [L.30.2.1(6); G.9.4(6); G.9.2]

For EIS specific measurements, compliance, and reporting of SLA metrics,

Quality planning and

management are specific duties of all AT&T management personnel, and execution of quality processes is the responsibility of the entire AT&T team. **Figure A-6.1-1** summarizes the following processes AT&T will implement to organize and manage quality for EIS:

- Aligning our baseline management and quality processes to the duties and responsibilities of our program management and CSO staff

- Identifying the SLAs specified for the EIS contract at RFP Section G.8 and the identification of the supporting KPIs and AQLs for each service covered by an SLA

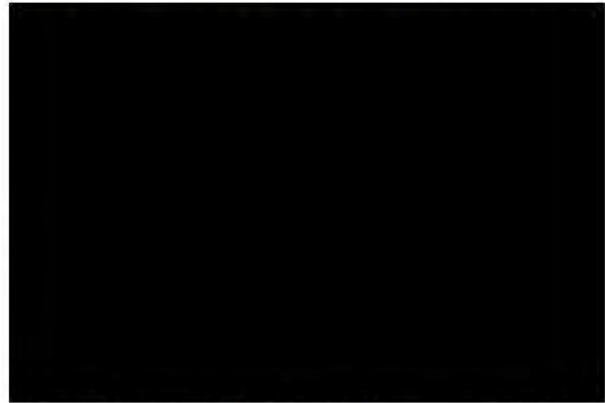
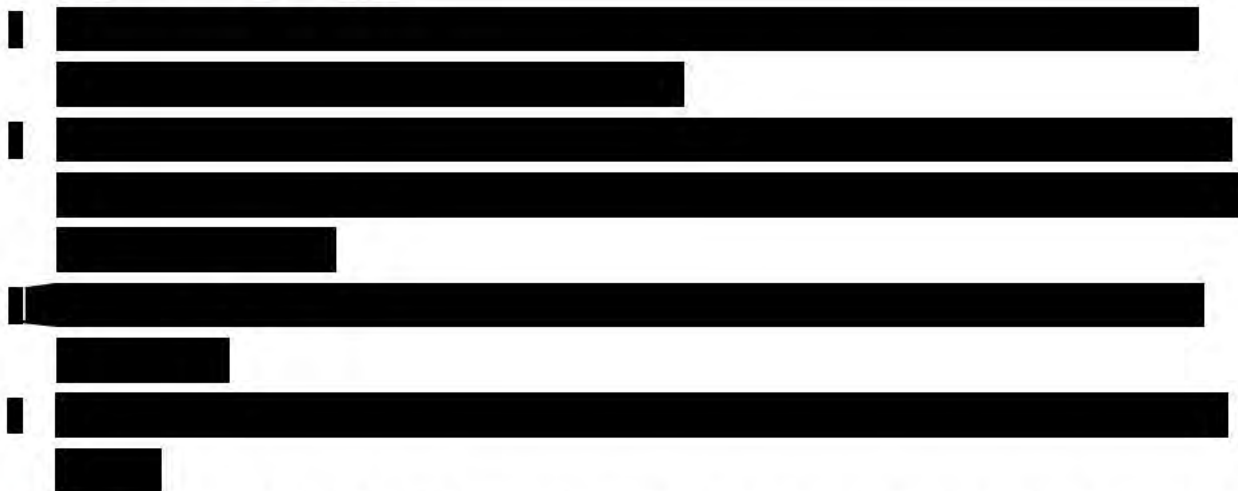


Figure A-6.1-1. AT&T Quality Management. GSA and agencies receive high quality deliverables with our disciplined QMS.

- Monitoring and managing performance against all contract performance requirements [G.9.2(2)]



- Submitting SLA data for performance monitoring and reporting to support accurate assessment of SLAs [G.9.2(1)]



- Working collaboratively to resolve all SLA issues with customer agency program managers and task order managers to continuously improve services and performance [G.9.2(4)]

A-6.2 Management Approach for Ensuring Compliance with Contractual Service Level Agreements (SLAs) [L.30.2.1(6); G.9.4(6)]

At the start of our EIS contract and at the start of each TO, we identify the applicable SLAs and their KPIs/AQLs for each service covered by an SLA. Our program manager establishes processes and reports for management and monitoring of service performance which provide needed information on a daily, weekly or monthly basis dependent on the sensitivity, response times, and past experience with performance on specific SLAs. These may consist of:

- Internal monitoring, measurement, and sampling processes/reports to capture performance statuses before they become non-performance issues
- Management discussions/meetings with agency TO project managers to review progress and identify any potential performance issues
- Programmed and random monitoring and sampling of targeted SLA performance between formal reporting periods
- Formally measuring and reporting on performance at specified intervals
- Identifying variances and developing plans to address them
- Applying credits per the credit formulas and processes established, when appropriate, for the specific failed SLA and the Service Level Agreement Credit Request (SLACR) processes

AT&T measures and samples performance throughout the reporting period, with emphasis on those services that are considered highly critical, have very small margins of error, or have had performance problems in the past [G.8.3.1]. Measuring and sampling during the performance period is done through a combination of data draws on specific services and managerial discussions with our CSO and agency-assigned project managers. At the end of each reporting period, the AT&T project managers use that data as part of their stewardship meetings with agencies where they discuss issues, identify trends and develop solutions.

A-6.3 Management Approach for Reviewing Work in Progress [L.30.2.1(6); G.9.4(6)]

The AT&T EIS program manager and AT&T TO managers will review work in progress and our customer service performance through multiple means:

- Routinely pulling reporting data for SLA performance and for other performance factors multiple times during the month to review and allow for the opportunity to address performance or service issues
- Routinely talking to customers, AT&T client executives, and GSA/agency staff to gather information about service performance and any concerns/issues that might need to be addressed, as well as leading practices and successes that can be shared with other customers and projects

A-6.4 Management Approach for Providing Customer Support Services [L.30.2.1(6); G.9.4(6)]

GSA and customer agencies will receive superior customer support services through the dedicated AT&T EIS CSO and the client executive teams working directly with agencies on each task order. The CSO, which is built upon years of lessons learned serving the Networkx contracts, is

discussed in detail in **Section 1.1.8**. Our systems and processes have evolved to best support EIS requirements now and will continue to evolve, as needed, throughout the life of the EIS contract. It is



Figure A-6.4-1. AT&T's Product and Service Assurance Team: Our dedicated staff provides GSA and Agencies expert quality monitoring support.

designed to provide the GSA and agencies fully-compliant, efficient service delivery and customer support. Our CSO's Product and Service Assurance team, **Figure A-6.4-1**, has staff specifically dedicated to managing performance and quality, supported by plans and processes designed to deliver optimum performance and service to our customers.

A-7 Key Personnel and Organizational Structure [L.30.2.1(7); G.9.4(7)]

GSA and customer agencies will benefit from the experience and subject matter specialization our team offers in managing all aspects of the EIS Contract. The quality of a service is often only as good as the people who support it. Even though we live in a world of rapidly expanding technology, the people that we work with and the organizations that support them are of utmost importance. In support of EIS, AT&T intends to keep our current Networkx team in-place, with whom GSA and agency

customers are already familiar. **Table A-7-1** provides the features and benefits of this approach.

Table A-7-1. AT&T Key Personnel and Capabilities. GSA and agencies benefit from a highly trained and experienced team of AT&T professionals.

AT&T Features	GSA and Customer Agency Benefits
Existing sales client executives and customer service program teams will continue to service and support individual agencies	Existing relationships and understanding of customer environments facilitate service support and efficiently address customer's mission objectives.
Extensive experience with large, global projects.	Agencies benefit from lower risk to their operations since experienced PMs with skills across the breadth of EIS services deliver transition. Agencies receive a superior customer experience, while completing projects within committed scope, budget and timelines.
Existing work center personnel already Homeland Security Presidential Directive (HSPD) cleared	Our available facility speeds operational readiness while maintaining highly secure physical and logical protection for agency location and data.
Personnel available to support agency specific projects requiring clearances (technical engineering specialists, feet on the street, Information Security, etc.)	AT&T's deep staffing bench allow us to assign specialized resources on-demand to support mission critical operations, including classified deployments, with reduced timeframes to start projects.

A-7.1 Management Structure, Organizations, and Roles and Responsibilities of Each Component That Performs Work Under the Contract [L.30.2.1(7); G.9.4(7)]

AT&T's management structure and EIS organization was formulated on the successes and efficiencies created from our [REDACTED]

Figure A-7.1-1

[REDACTED] comprises the support needed to properly address GSA program requirements, manage overall contract performance, and provide the infrastructure necessary to properly respond to agency-specific needs and missions.

Designed to quickly and efficiently respond to requirements, our structure is lean, with our Program Manager, [REDACTED] reporting directly to the EIS Operations Manager [REDACTED] our key person on EIS, will work directly with the GSA EIS Program Management Office (PMO) and manage the AT&T Customer Support Office, our companion to the PMO. Aligned with [REDACTED] are AT&T's Client Executive Teams that focus exclusively on the needs of customer agencies. By coordinating the objectives of the GSA EIS PMO with customer agency network, IT, and mission needs, [REDACTED] will create the synergy needed to accomplish a smooth migration from Networx to EIS.

Shown in the bottom half of **Figure A-7.1-1** are the functional organizations performing work under the EIS contract. Strategic areas requiring primary points of contact are defined by an asterisk. A description of each organizational component is provided in **Section A-7.2** along with a listing of our strategic POCs and their associated responsibilities.



Figure A-7.1-1. AT&T Customer Support Office.

A-7.2 Key Personnel and Corporate Structure [L.30.2.1(7); G.9.4(7); H.10]

Our Program Manager and a link to our external website, shown in **Table A-7.2-1** **shows** our primary points of contact that support our organizational structure. These functional specialists are important to the overall success of our CSO and provide GSA and the agencies a combined understanding that exceeds 50 years of direct Networkx and LSA experience. These specialists will support agencies with the transition to EIS with minimal risk and without performance degradation.

Table A-7.2-1. Subject Matter Specialists. AT&T's EIS organization provides Points of Contact with hands-on understanding of the functional domains, agency priorities, and program objectives.

EIS Organization: Program Functions, Descriptions, and Personnel				
Function	Role & Responsibility	Name	Telephone	Email
Program Management				



EIS Organization: Program Functions, Descriptions, and Personnel				
Function	Role & Responsibility	Name	Telephone	Email
EIS Key Contacts				

A-7.2.1 Key Personnel [L.30.2.1(7); H.10.1 – H.10.1(d)]

The AT&T EIS Program Manager (PM), [REDACTED] is proposed as the key person assigned to the EIS contract.

A-7.2.1.1 EIS Program Manager [H.10.1(a-d)]

[REDACTED] of AT&T experience. Additional resources, while not named as Key Personnel, are important in support of the EIS contract and will be named within the Points of Contact.

As EIS Program Manager, [REDACTED] is responsible for all AT&T performance elements on the contract and will work within AT&T on resource adjustment as necessary. A summary of her experience and her EIS responsibilities are listed in **Table A-7.2.1-1**.

Table A-7.2.1-1. [REDACTED] and EIS Program Manager Responsibilities. [REDACTED]

A-7.2.1.2 Other Personnel AT&T Considers Important to the Overall Operation and Success of the EIS Contract [H.10.1]

Our important points of contact for overall operation and success of the EIS contract are shown in proposal **Section A-7.2, Table A-7.2-1**.



A-7.2.1.3 Substitutions and Additions of Contractor Key Personnel [H.10.2]

In the event of substitutions or additions to key personnel, AT&T will submit resumes for the written approval of the GSA CO. AT&T will not substitute its key personnel during the first 180 days of EIS performance except under exceptional circumstances (e.g., illness, injury, termination, etc.) and when approved by the GSA CO. After the initial 180-day period, AT&T submits all proposed substitutions and additions to the GSA CO in writing 15 days (30 days if security clearance is required) prior to the anticipated effective date of the proposed personnel change. For all proposed changes, AT&T will certify that the proposed replacement is better qualified, or at least equal to, the key personnel to be replaced and provides the GSA CO with a detailed explanation of the circumstances requiring the personnel change and the complete resume(s) for those proposed replacement personnel.

A-7.2.2 Corporate/Organizational Structure [L.30.2.1(7); H.10.3]

To accomplish EIS management and oversight responsibilities, the PM is supported by a Networx-proven organization that is discussed throughout this PMP.

A-7.2.2.1 Charts That Show the Functional Relationships Among Organizational Elements and Identify the Positions of Key Personnel Assigned [H.10.3.a]

The Customer Support Office (CSO), led by our PM [REDACTED] is the operational engine driving our EIS performance. As shown in **Figure A-7.2.2-1**, the functional groups, organized along administrative lines similar to those used on Networx, have clearly defined areas of responsibility that work together providing an effective, user- friendly EIS experience for GSA and client agencies.

The AT&T EIS CSO is located in AT&T facilities and is fully operational and dedicated to facilitating client agencies use of the EIS contract. This support includes but is not limited to providing product and service information, sales, order processing, implementation, billing, customer service, training, inventory management, responding to service inquiries, dispute resolution, and reporting.

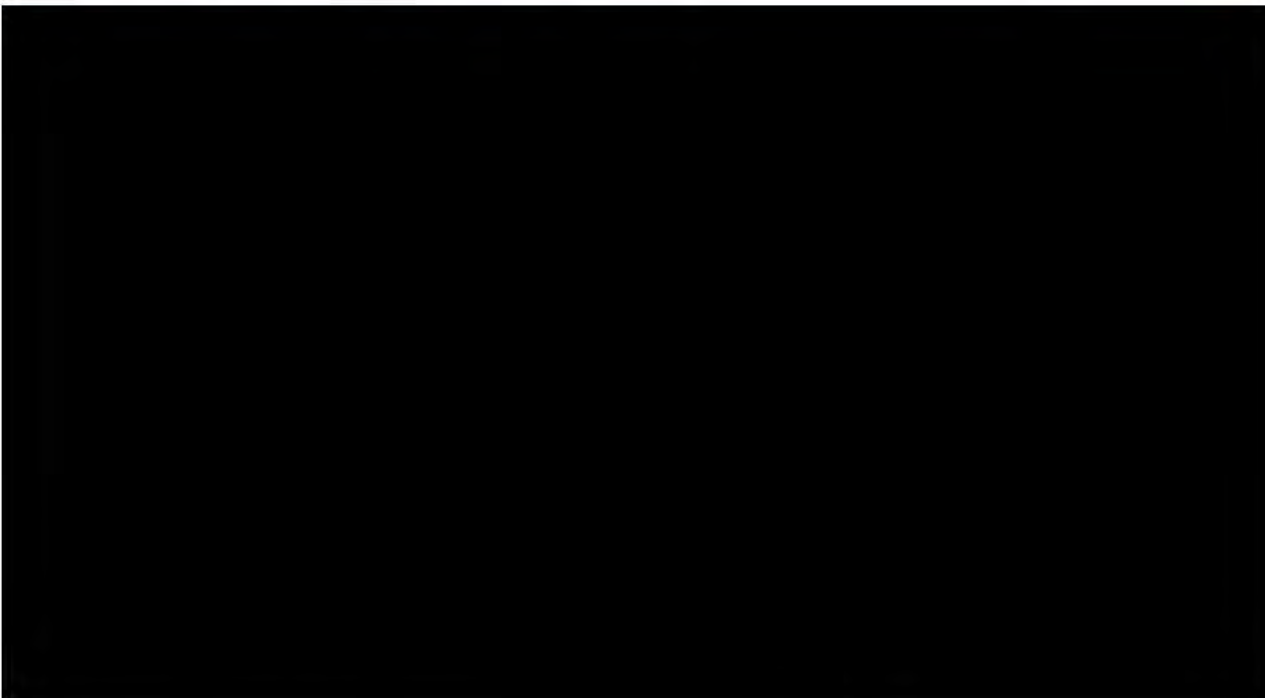
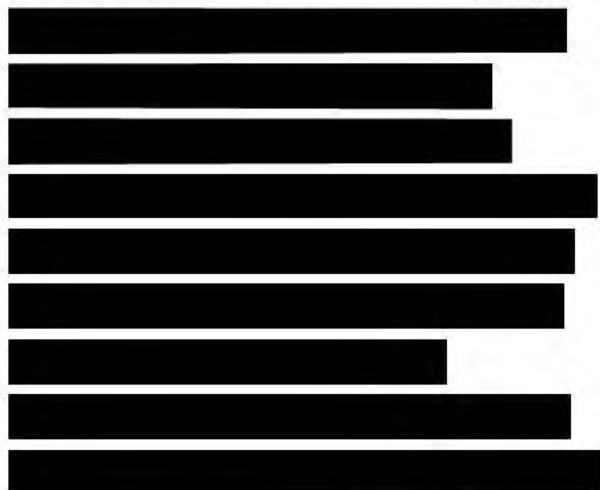


Figure A-7.2.2-1. Functional Relationships Among Organizational Elements.

A-7.2.2.2 Relationship of the Highest-Ranking Individual Assigned to the Contract to the Corporate Chief Operations Officer, President, and Chief Executive Officer [H.10.3.b]

As depicted in Figure A-7.2.2-2,



This access to corporate resources and decision makers enables strong and focused EIS program support.

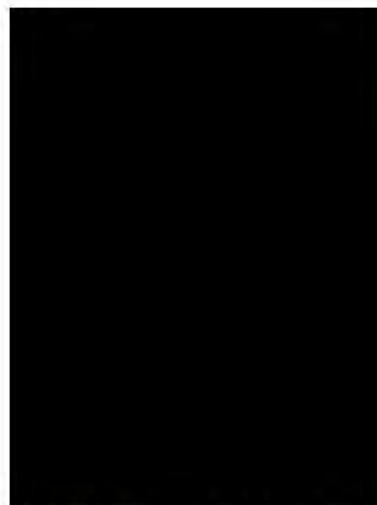


Figure A-7.2.2-2. Corporate Relationship Structure.

A-7.2.2.3 Organization Charts and Plans That Clearly Depict the Areas of Responsibility and Flow or Authority between AT&T and Its Subsidiaries and/or Major Subcontractors [H.10.3.c]

Our subcontracting plan for EIS applies strategic sourcing processes already in place and used successfully on Networx, the LSAs and multiple other contracts.

Figure A-7.2 -1 depicts the relationship of our subcontracts group within our CSO. Our plan includes subcontracting to reliable AT&T vendors inclusive of systems integrators, suppliers, and small businesses, and identifying subcontractors to provide capability (not organic to AT&T) as part of an integrated solution. AT&T confirms that only qualified subcontractors are engaged on the EIS contract through rigorous qualification, selection, and performance monitoring processes.

The business operations functional group of the CSO is responsible for managing our contracts and subcontracts planning and operations with the support of AT&T's corporate vendor management team. **Figure A-7.2.2-3** details our strategic sourcing process and the flow of authority between AT&T and our subsidiaries and/or major subcontractors.

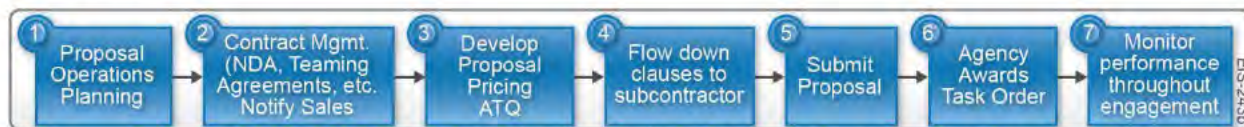


Figure A-7.2.2-3. Subcontractor Strategic Sourcing Process. *Our plan integrates subcontracting throughout the solution lifecycle.*

Our subcontractor qualification review includes a risk assessment analysis (e.g., financial and sustainability screenings, quality reviews, etc.), a market scan for emergent technology providers that may augment available service or product portfolios, and agency-driven “best fit” assessments. AT&T also selects subcontractors to meet EIS contract and agency-specific small business requirements. All AT&T subcontractor agreements for EIS are managed through the AT&T consolidated Corporate Vendor Management organization, which monitors and evaluates performance metrics for each subcontractor through the life of the EIS contract.

A-7.2.2.4 Charts and Description Text Indicating the Contractual, Technical, and Administrative Interfaces between the Government and AT&T, AT&T's Subsidiaries, and Major Subcontractors [H.10.3.d]

The dotted arrows in **Figure A-7.2.2-4** below depict the contractual, technical, and administrative interfaces between AT&T, GSA, and the EIS participating agencies (we are not proposing major subcontractors for the EIS contract). When individual federal agencies order services through the EIS contract,



Figure A-7.2.2-4. Interfaces between Government and AT&T.



they receive customer and administrative support from the CSO and direct operational support from implementation and service teams backed by AT&T support organizations.

Coordination and Communication [G.9.3(1-8)]

Consistent and effective communications between AT&T and government management and technical personnel are essential to the success of the EIS program. The orange arrows in **Figure A-7.2.2-5** illustrates the open lines of communication AT&T will use to coordinate EIS contract activities.

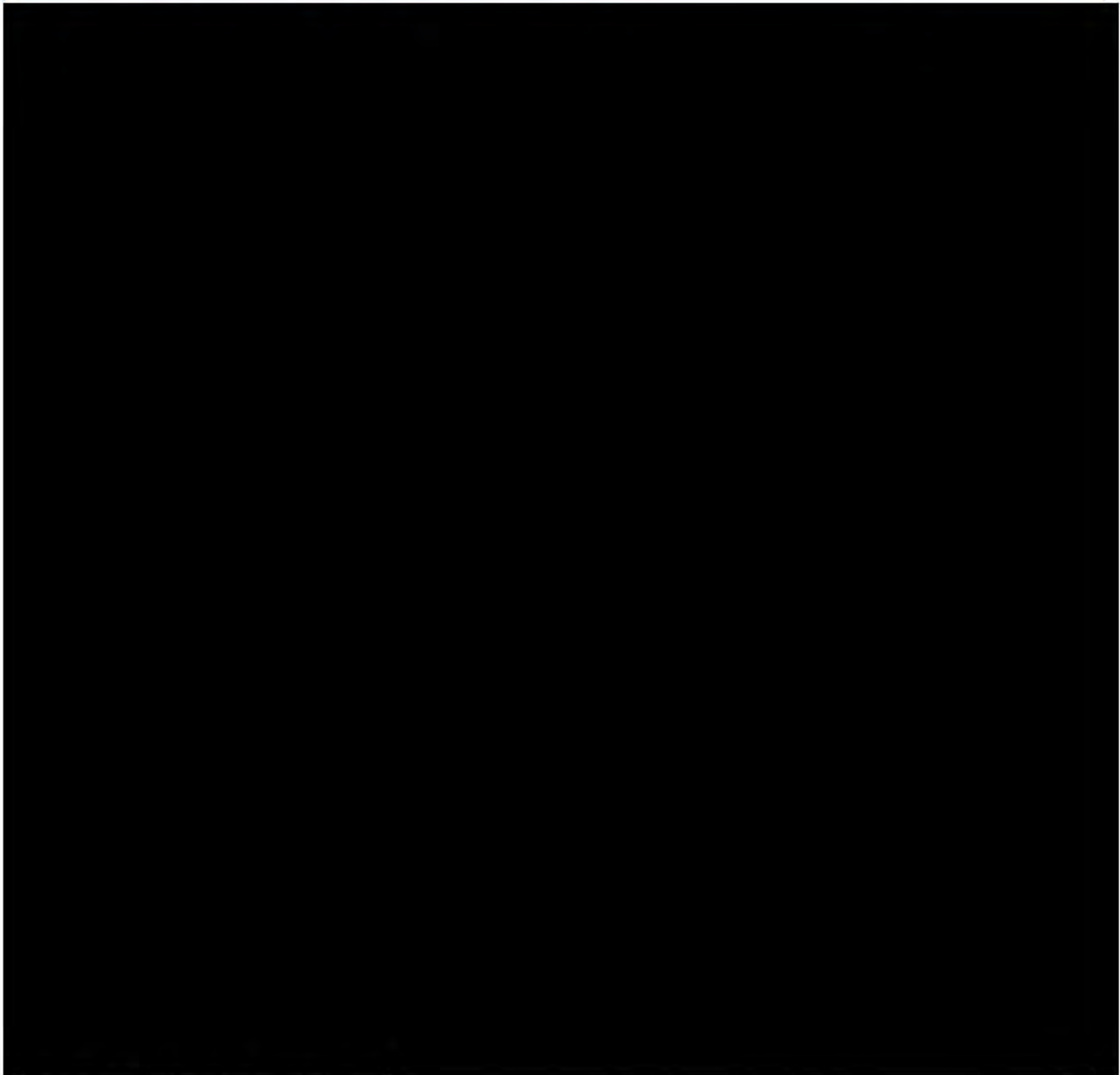


Figure A-7.2.2-5. CSO Organization.

Our CSO helps facilitate communication and is available to the government on a 24x7 basis throughout the life of the contract. **Table A-7.2.2-1** provides a proposal reference that addresses each of the solicitation requirements.

Table A-7.2.2-1. AT&T's Coordination and Communications. AT&T is organized to provide responsive, designated POCs resulting in streamlining operations and quick resolutions.

RFP Reference	Cross Reference Section
Communications Between Management and Technical Personnel [G.9.3(1)]	As depicted in Figures A-7.2-4 and A-7.2-5 , AT&T will implement a consistent and effective communication process between management and technical personnel.
AT&T Management of the Customer Relationship [G.9.3(2)(a-f)]	The CSO and Client Executive personnel have primary responsibility to support the customers. Communication paths

RFP Reference	Cross Reference Section
	are indicated in Figure A-7.2-5 . Trouble Management is discussed in detail in Management volume Sections 1.1.4 and 1.1.5
AT&T Provision of Technical Expertise [G.9.3.3]	AT&T has bid all but 3 of the requested EIS Services. We have technical specialists for each of those services support the CSO and the EIS contract.
Response to EIS PMO Questions and Issues [G.9.3.4]	As discussed in this PMP and Management volume Section 1.1.4 the AT&T EIS CSO is responsible for full communications with the GSA PMO.
Escalation Procedure [G.9.3.5]	Discussed in the proposal section paragraph A-7.2.2.5
AT&T Capability and Authority [G.9.3.6(a-i)]	AT&T has full capability and authority to support all requirements on the EIS contract. The specific requirements listed in RFP G.9.3(6) are discussed throughout the Management Volume
AT&T Points of Contact List [G.9.3.7(a-k)]	We have provided initial POCs with this proposal in Table A-7.2-1 . Any modifications will be included in the formal submittal that will be provided to the government within 30 days of award.
Security POCs [G.9.3.8(a)]	AT&T security staff within our CSO is responsible for processing applicable personnel IAW FAR 52.204-9 as shown in Table A-7.2-1 .
POCs That who Have Passed National Agency Checks or Background Investigations [G.9.3.8(b)]	A POC listing and clearance levels for AT&T personnel on EIS will be provided to the Government IAW RFP Section G.9.3.8(b) no later than (NLT) 30 days after contract award.

Contract Administration [L.30; M.2.2; G.2]: AT&T contract administration activities:

- **Government Points of Contact [G.2.1]:** AT&T has successfully worked with our government counterparts throughout the contract administration of the existing Networx and regional contract programs. In preparation for transition to EIS, our contract manager, who has extensive experience with the Networx contract, will support EIS, including working with the GSA Contracting Officer (CO), Contracting Officer's Representative (COR) as required, and those personnel named as an Ordering Contracting Officer (OCO) as a result of Delegations of Procurement Authority (DPA). To fully comply with and understand government requirements for EIS, we have reviewed each of the government roles and responsibilities as defined in RFP Sections G.2.2 through G.2.2.2.5.
- **BSS Final Contract Acceptance [G.2.3; E.2.1; H.3]:** AT&T has provided a Draft BSS Verification and Test Plan as **Appendix C** to our Management Proposal that describes our approach to pass the required tests within 12 months from the acceptance of the final plan. We understand we need to pass these tests within 12 months, unless the government causes delays, or GSA may cancel our contract and

we would not receive the Minimum Revenue Guarantee nor be able to make any financial claim or request for settlement if we fail to pass the tests.

- **Contract Modification [G.2.4; J.4]:** AT&T has extensive experience in modifying the Networx Universal and Networx Enterprise contracts. Our dedicated team has worked closely with GSA to execute more than close to [REDACTED] modifications covering approximately [REDACTED] proposal submissions. As a result, agency users have been able to use the most current commercially available services at competitive prices over the term of the contracts. AT&T will apply this contractual model to future EIS modifications, working with our customer agencies and the GSA, throughout the full period of performance.
- **Contract Closeout [G.2.5]:** AT&T is familiar with the requirements Federal Acquisition Regulation (FAR) 4.804 and General Services Acquisition Manual (GSAM) Subpart 504.804-5 and routinely works with COs to close out contracts and delivery orders for communications services. Our enhanced BSS processes for receiving and monitoring task order performance and invoicing under the EIS contract will facilitate close out activities, with the required documentation readily available.
- **Past Performance [G.2.6]:** AT&T is vigilant in monitoring our contract performance and identifying areas for continuous improvement in schedule, quality, and cost. Each past performance assessment score provided by the government that is less than “exceptional” will be assessed by our project and contract personnel for methods to improve our overall contract and TO performance. Grading that falls below our acceptable performance standards requires a plan of action for performance improvement that will be implemented by our TO project managers.
- **Program Reviews [G.9.6]:** AT&T’s EIS CSO includes staff dedicated to program management review and reporting. This provides GSA with responsive, informed support by staff with continuity and complete understanding of government reporting requirements, priorities, and topics of interest to the agencies.

The AT&T Quarterly Program Management Review Process is shown in

Figure A-7.2.2-6. The Quarterly Program Management Review is attended by the GSA

PMO and AT&T's EIS CSO, along with functional and management staff from both organizations to provide in depth discussion on any specific topics of interest for that quarter. Data is presented to the Government in a consistent presentation format, and also briefed as an oral presentation allowing for Questions and Answers and follow-up discussion between both parties as necessary.

Quarterly Program Status Report

[G.9.6.1]: AT&T will deliver compliant Quarterly Program Status

Reports to the GSA PMO and will lead Quarterly Program Management Review meetings. **Table A-7.2.2-2** shows our quarterly status reports, the information sources for those reports, and the AT&T functional staff responsible for preparing the report.

Table A-7.2.2-2. AT&T Quarterly Program Status Report Elements and Functional Areas Supporting Each.

Figure A-7.2.2-6. Quarterly Review Process.

A-7.2.2.5 Description of Corporate Escalation Procedures for Resolving Critical Issues, Including Points of Contact [H.10.3.e]

The GSA EIS Client Executives escalate critical issues directly to the AT&T EIS PM, [REDACTED] as shown in **Figure A-7.2.2-7**. If executive level escalations are required, they are initiated with [REDACTED]

President Public Sector & FirstNet.

GSA or customer agencies may request an escalation at any time

through their specific client executive as appropriate. Specific to service impacts, customer agencies also have access to AT&T's web-based digital first platform and toll free phone number. AT&T's global maintenance work centers maintain internal protocols for escalating service outages (based on criticality) and for notifying management, as needed.

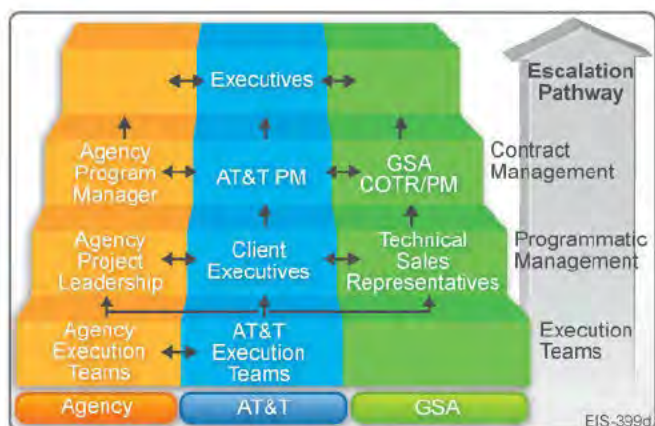


Figure A-7.2.2-7. EIS Escalation Pathways.
Multiple escalation pathways expedite issue resolution.

A-8 Risk Management [L.30.2.1(8); G.9.4(8)]

GSA and customer agencies will receive a proactive, comprehensive, and realistic risk management solution that is structured to control technical and management risks across all EIS contract functions. Risk is inherent in significant undertakings such as roll out and management of technology infrastructure needed to support critical mission functions. What differentiates a successful project from a disastrous one is how well risk is identified, understood, and addressed. A provider who has successfully managed risk end-to-end for enterprise-wide implementations, a wide spectrum of solutions, and diverse geographies will deliver a least-risk pathway to success.

The AT&T risk management process is based upon constant vigilance enhanced by improvements from lessons learned across our experience, specifically those gained from similar GSA programs including Networx Universal, Networx Enterprise, Alliant, Connections II, and SATCOM II. Our risk process is fully compliant with the needs of the EIS contract and will provide best-in-class risk identification and mitigation throughout the life cycle of the contract.

Did You Know?

AT&T's risk management lessons learned are resultant from performing similar services for over 6 GSA contracts.

Our core risk management process, shown in **Figure A-8-1**, provides an overview of the methodology applied from initial risk identification through mitigation and final resolution. Our risk management tools, shown in green, are the foundation behind our process. Each of our risk and project managers is trained internally on these tools at no additional charge to the government, which helps maintain our focus on risk avoidance, early detection, and resolution. The AT&T risk management process also applies to EIS cloud computing risk requirements outlined in **Appendix E**. The AT&T risk management process and overall approach are applied to all TOs, project plans, transition scheduling, and throughout system operations. We also place significant emphasis on risk identification and mitigation when installing new services. This helps provide each agency continuity of service to support their mission without experiencing performance degradation due to unforeseen risks.

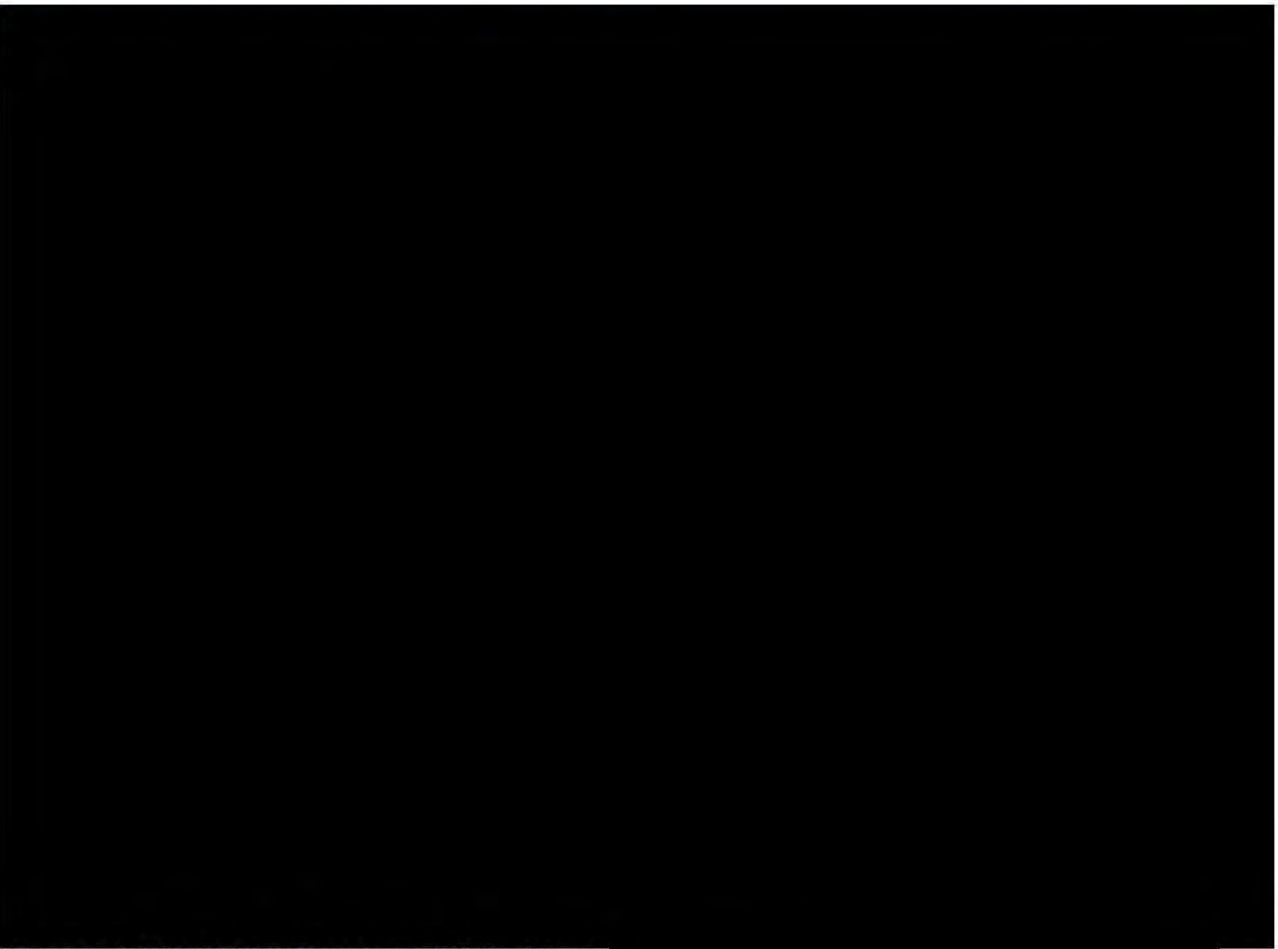


Figure A-8-1. AT&T Risk Management Methodology.

Table A-8-1 summarizes the features of AT&T's EIS program's risk management process and the related benefits derived by GSA and customer agencies.

Table A-8-1. AT&T Risk Management Process Features and Benefits. *GSA and customer agencies receive a rigorous risk process from AT&T that mitigates performance concerns and helps them achieve important mission objectives.*

Features	Benefits
AT&T risk identification, assessment, and mitigation approach is based on our long legacy working with GSA on regional, Networx, Alliant, and other federal programs within AT&T and lessons learned from our commercial customers.	
AT&T risk management database contains potential risk areas (lessons learned) for avoidance gained from like GSA programs and technical and management operations.	

Features	Benefits
AT&T's project team, including subject matter specialists is thoroughly trained on risk identification, risk analysis, and risk mitigation	
AT&T's principle MS Excel risk management tool, has dashboard capability to identify the total number of risks identified on a project, criticality of risk, status of mitigation, and reporting capability for our Program Manager and Risk Manager	

A-8.1 Process for Identifying Program Risks, Including Risks Identified in the Contract and Actions to Mitigate them [L.30.2.1(8); G.9.4(8)]

AT&T employs a structured, repeatable process for risk identification and mitigation beginning with risk identification and ending with risk resolution and documentation. Each step within the process has clearly defined roles and responsibilities. We outline EIS program-related risk activities and organizational responsibilities in **Table A-8.1-1**. Example EIS risks and associated mitigation actions are contained in **Table A-8.1-5**.

Table A-8.1-1.The AT&T High-Level Process for EIS Program Risk Identification and Mitigation. *Network-proven, documented, interactive processes minimize implementation and operational risks for GSA and agencies.*

Activity	Performed by	Description
Risk Identification	Stakeholders	Stakeholders identify and report a potential risk or issue. Stakeholders include, but are not limited to, members of the program team, GSA, the agency stakeholders, contractors, vendors, or internal and external oversight bodies
Risk Assessment/Analysis	Risk Manager/ Risk Owner	Estimate the probability of occurrence and the magnitude of impact for each risk event. Prioritize risks dependent on probability, impact, and timeframe. Figure A-4.1.4-1 . Principle Transition Risks Register, in Section A-4 above provides a good example of a well-constructed risk analysis.
Risk Planning	Risk Manager/ Risk Owner	Develop mitigation strategy/contingency plan with GSA and agency representatives
Risk Mitigation	Risk Manager/ Risk Owner	Execute the developed plans. Take the steps necessary to reduce adverse effects
Risk Monitoring/ Tracking	Risk Owner	Risk is logged upon identification and is tracked against magnitude and resolution execution throughout the process
Close Risk	Risk Manager	Once the Risk Manager decides a risk has been addressed and resolved, it will be closed and a record of the risk's history is retained for lessons learned

The risk identification process includes the involvement of GSA and agency personnel along with our AT&T risk management team. This coordinated approach reduces the possibility of potential risks from being identified too late, causing significant concerns. **Table A-8.1-2** outlines the AT&T risk management team and associated responsibilities.

Table A-8.1-2. AT&T EIS Program Risk Management Team. *The EIS Risk Management Team provides leadership and an integrated organizational approach to maximize identification, mitigation, and resolution of risks.*

AT&T Team Member	Role/Responsibilities
EIS Program Manager	- Stays apprised of major risk areas and schedule for resolution - Communicates significant issues to GSA/agency contracts & management team - Coordinates internal requirements necessitating corporate AT&T executives
Risk Manager	- Administers for all aspects of risk management - Leads and participates in the risk management process - Takes ownership of the risk mitigation/contingency planning and execution - Makes the final decision on risk actions in coordination with GSA and agencies - Assigns authority to execute the Risk Management Plan to the Team Risk Manager
Team Risk Manager	Manages the execution of the Risk Management Plan per the Risk Program Manager's delegation
Project Managers and Team Leads (e.g., Network Engineer, Security Engineer, Quality Manager)	"Owns" the risk associated within their span of control - Provides the first line of management supervision - Oversees and manages all aspects of the technical delivery and performance - Identifies risks in their area of control - Plans risk mitigation development - Logs and tracks risk - Monitors risk - Reports Risk escalation
Program Master Scheduler	- Conducts a scheduled risk assessment for each control area and for the total program - Uses specific tools such as the critical path methodology in performing the risk assessment - Provides critical assessment of program risks based IMS

When a potential risk event or series of risk events has been identified and documented, the risk will be further analyzed. Risk analysis involves determining the probability of occurrence and the expected financial impact of the event to the program. During risk analysis, each potential risk event is analyzed for:

- **Probability of Occurrence.** The likelihood that the risk will occur. Probability is expressed as high, moderate, or low.
- **Impact of Risk.** The impact of the risk if it occurs. This is the magnitude of consequences if the risk event occurs. Impact is expressed as high, moderate, or low. Impacts can be assessed against program mission, expense, schedule, scope, and/or quality.

Probability and impact will be assigned a color code for managing prioritization as depicted and defined in **Table A-8.1-3.**

Table A-8.1-3. AT&T Analysis Process.

When prioritizing risks, qualitative scoring facilitates management review, oversight, and action by rank ordering the risks into one of these three ratings. This prioritization will ascertain which risks require significant time and effort for remediation steps and risk mitigation actions. Higher priority risks will receive more attention during weekly project reviews than lower priority risks. AT&T's risk mitigation steps are outlined in

Table A-8.1-4.

Table A-8.1-4. AT&T's Risk Mitigation Steps. *AT&T uses a structured set of risk mitigation steps that begin from developing the mitigation plan to closing the risk.*

Activity	Performed by	Description
Risk Mitigation Plan Development	Risk Manager/ Risk Owner	- For risks determined to have a probability of occurrence that is at least likely to occur or with at least a moderate impact level, the Risk Mitigation Plan defines activities to be performed or the steps to be taken to keep the risk from negatively impacting the program - Once program management has categorized and recorded the risk in the Risk Management Tool spreadsheet, a proper response strategy is identified, based on the probability, severity, and timeframe of the risk - The higher the probability and impact of the risk, the higher priority it receives. High priority risks are assigned to a risk-specific Risk Owner who assumes responsibility for the risk while working with the Risk Manager and the program team to execute the mitigation strategy
Log and Track Risk	Risk Owner	- Identified risks are logged and regularly tracked for continual assessment in a Risk Progress Report. The Risk Progress Report will include the following information for each risk: - Control Number (Risk Identification Number) - Description - Date Entered - Date Identified - Planned Resolved Date - Risk Owner - Probability (H – High, M - Moderate, L - Low) - Impact (H – High, M – Moderate, L - Low) - Status (Green, Yellow, Red) - Strategy for Mitigation
Monitor Risk	Risk Owner	Once a Risk Mitigation Plan has been created for an identified risk, the risk is logged in the Risk Progress Report, which is also referred to as the Tracking Report. The risk is then tracked using the risk management tool spreadsheet
Risk Escalation and Reporting –	Risk Owner	Risk Owners will manage their respective risks within Risk Summary Reports. They will update the Risk Management Tool spreadsheet accordingly. Status of all risks is monitored by the Risk Manager. The status of program risks in the Risk Management Tool spreadsheet is regularly reported during monthly operations review meetings using the risk Progress Report.

With ongoing technological convergence, a mature risk management approach is critical to supporting business continuity throughout GSA and the agencies. Potential EIS risks and actions to mitigate them are shown in **Table A-8.1-5**.

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

Functional Areas Within EIS	Potential EIS Risk Areas	AT&T Actions to Mitigate Them

AT&T provides GSA and the agencies program experience, in-place risk processes, and a corporate emphasis on risk avoidance. Together they minimize program disruptions, increase agency confidence levels, and accelerate implementations.

A-9 Information Systems [L.30.2.1(9); G.9.4(9)]

GSA and agencies will benefit from an EIS BSS that consists of a number of integrated subsystems that implement the requirements of the EIS contract. We design, develop, test, deploy and maintain BSS to be consistent with EIS security requirements, particularly the need to prevent unauthorized access to the government's data. To this end, we will use Two Factor Authentication (2FA) to control entry into our portal, Business Center, which allows authenticated users to access BSS functions within our Government Center. We will use RBAC to prevent an agency's access to data belonging to any other agency. In fact, we currently use RBAC to restrict a user's access to data, or functionality, to those authorized for the contractual role in which that user works for the government.

At that start of a TO, we work collaboratively with the COR to customize a standard set of EIS roles to meet the requirements of the TO and define the access authorizations for that role. These fine-grained permissions control the user's access to the BSS functions of Service Ordering, Inventory Management, Billing, and Service Management (**Section A-2** and **Section 1.1.3** provide further details on the operation of the BSS). The permissions further control the user's access to specific data elements. BSS does this by mapping the physical schema of data elements in BSS databases to the logical schema of data elements authorized for the user role in question. Depending on TO requirements, we can provide further protection by restricting the database functions of update, insert and delete to authorized user roles.

A-9.1 Description of the BSS Employed to Implement the Requirements of the Contract [L.30.2.1(9); M.2.2(3); G.9.4(9)]

AT&T applies a set of time-tested standards and a disciplined approach to the design, development, testing, deployment, operation, and maintenance of the BSS employed to implement the requirements of the EIS contract. AT&T Agile software methodology is used to develop and support our BSS providing faster implementation of future enhancements while controlling performance risk.

AT&T provides a specific and effective approach in support of GSA and agencies from our Contractor Data Interaction Plan (CDIP) in **Section 3** [M.2.2(3)]. Our CDIP is fully compliant with the RFP CDIP requirements.

Our BSS target platform architecture, as seen in **Figure A-9.1-1**, uses a layered Application Programming Interface (API) based architecture.



Figure A-9.1-1. AT&T BSS Architecture.

With respect to implementing the contract-required information security controls, we overlay design, development, and implementation with the Risk Management Framework (RMF), described fully in the BSS RMF Plan submitted as part of this

proposal and illustrated in

Figure A-9.1-2. AT&T Security Policy and Requirements (ASPR) provide a security framework that is adopted from the beginning of the development process. The BSS will comply with the EIS security requirements specified in G.5.6.

The purpose of employing the RMF is to integrate information security controls and activities throughout the life cycle to provide

information systems with sufficient, risk-based, and ongoing security. In applying the RMF to the BSS, we comply with the current applicable federal and agency-specific IT security directives, standards, policies, and reporting requirements to assess the direction of a project throughout the development lifecycle. Those include the relevant GSA IT Security Procedural Guides and National Institute of Standards and Technology (NIST) Special Publications (SP), including 800-53, rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, 800-34, *Contingency Planning Guide for Federal Information Systems*, and 800-37, rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, among others.

A-9.1.1 Consistency with Security Plans to Prevent Unauthorized Access to the Government's Data [L.30.2.1(9); G.9.4(9)]

The BSS is designed and engineered to implement security controls required for a Moderate Impact system by GSA's IT Security Procedural Guide: *Access Control*, CIO-IT Security-01-07, and NIST SP 800-53, rev 4, including the access controls. Within the context of preventing unauthorized access to government data, the BSS design and development process includes activities and controls such as those summarized below:

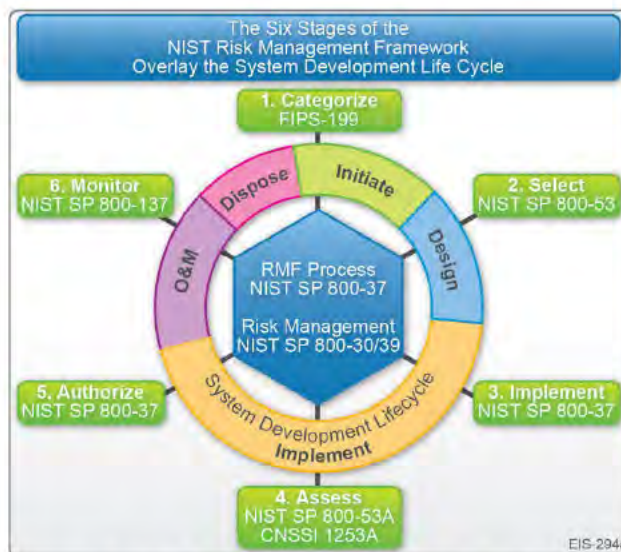


Figure A-9.1-2. AT&T's RMF Life Cycle.

Properly implemented, the RMF synchronizes information security with system development and maintenance, resulting in more thorough and economical compliance throughout the life cycle.

- Identifies the impact level of the information being processed based on the guidance in FIPS 199, Standards for Security Categorization of Federal Information and Information Systems. GSA determined the security category of the BSS and the information that it stores, processes, and/or transmits to be Moderate Impact in accordance with FIPS 199.
- Identifies, integrates, and validates the Moderate Impact controls consistent with control requirements in the applicable GSA Procedural Guides and NIST SP 800-53, rev 4. This includes verifying that access controls and identification and authentication (I&A) controls are planned, engineered, and implemented in the BSS.
- Employs FIPS 140-compliant encryption for data transmitted between agency customers and the BSS.
- Identifies all user inputs and system entry points so that safeguards can be designed to minimize risks and vulnerabilities from hostile inputs.
- Validates that all databases containing government information are protected from unauthorized access within the AT&T Intranet.
- Validates that there are mechanisms that protect the BSS from known vulnerabilities that could enable unauthorized access, such as buffer overflow, SQL injection, cross-site scripting, and denial-of-service attacks.

Appendix G describes how AT&T develops the BSS System Security Plan (SSP). The SSP identifies the controls implemented to prevent unauthorized access, such as those summarized above, and describes how AT&T implements those controls. AT&T tests the controls through the initial BSS Assessment and Authorization (A&A) and thereafter through continuous monitoring.

AT&T strictly enforces measures to prevent access to government data by unauthorized internal users. We restrict access to authorized users and grant access only after we confirm that each user meets the HSPD-12 suitability requirements. Further, we enforce *least privilege* whereby users' access is restricted to the minimum required to carry out their assigned duties, and we maintain strict segregation of duties.

Access to all BSS functionality is via the Business Center portal as described in the BSS SSP. AT&T's Business Center enforces two-factor authentication and restricts

BSS user access to that which they are authorized. Each authorized user's permission levels restrict the user to applications, functions, and data based on RBAC controls. The permission levels are granular enough to confirm that users can only view and operate on the data for which they have been authorized. This prevents authenticated users from accessing data that they are not authorized to access.

AT&T BSS security is designed and implemented on all platforms (mainframe and midrange) at different resource layers — operating system/file system, application and database layers. The security layer of each application is carefully analyzed to determine what security controls are required to provide adequate protection for data and resources.

Granting access to any layer of a BSS application is strictly governed by a well-defined process that is subject to approvals by a designated approval hierarchy including final approval by the AT&T ISSO and bi-annual reviews. AT&T access procedures prevent any person, regardless of his/her level, to self-approve his/her access request. Periodic reviews are conducted by the AT&T ISSO with an escalation policy in place to address any variance or non-compliance.

BSS application resource administrators implement a security audit logging capability consistent with our security audit log review plan. The plan includes the following specifications that support preventing unauthorized system access:

- The frequency for security audit log review based on criteria such as system criticality, business/mission risk, expense, and system classification.
- The minimum unusual activities to be reviewed include multiple unsuccessful login attempts, user attempts to access files or resources outside their privilege level, and network activity.

Resource administrators perform the activities outlined in the security audit log review plan. Where the security audit log review is automated, anomalies in the security audit log are alarmed.

Resource administrators confirm that the access level assigned to each individual user account on the resource are appropriate and that each user's continued role

membership is appropriate. Resource administrators support user account access reviewers and security assessors to confirm that an individual's access is appropriate. Access to internal AT&T users or external customers is granted subject to the access and authorization policy and controls described above and recorded in an authorization database. Access to any data or resource is available through the BSS application only after the application determines the authorization level of the user from the authorization database.

In addition, the strict design principles consistent with the GSA Security Procedural Guides and NIST guidance help prevent any unauthorized users from accessing government data.

A-9.1.2 Consistency with Security Plans to Prevent Access by An Agency to Data Belonging to Any Other Agency [L.30.2.1(9); G.9.4(9)]

The same NIST-based access and I&A controls and RBAC that enforce least privilege and separation of duties among individual customer agency users enforce inter-agency separation. Role-based access control policies are coupled with access enforcement mechanisms to prevent access by one agency to data belonging to another agency.

A-9.2 Description of How AT&T Will Ensure Systems Are Available to Meet the Requirements of Business Support Systems [L.30.2.1(9); G.9.4(9)]

AT&T provides BSS availability by deploying a contingency planning process that integrates NIST SPs 800-53, rev 4, and 800-34 guidance for the Business Impact Assessment (BIA) and Disaster Recovery Plan (DRP) with the Contingency Plan (CP) and related processes and GSA's guidance, such as the IT Security Procedural Guide: *Contingency Planning (CP)*, CIO-IT Security 06-29. Controls include the plans themselves, alternate storage and processing sites, provisions for alternate telecommunications services and communications protocols, and software and data backups and recovery testing. To mitigate the consequences of disastrous events and restoring computing systems in support of business processes, all BSS applications must have:

- Application Impact Analysis (AIA) performed prior to solution design
- Solution design for DR to meet Recovery Time Objective (RTO)
- Deployed appropriate Recovery Type (RT)

- DRPs for recovery of system, database, and application
- DRP reviewed and updated annually or when there is a system change that requires a plan update

BSS availability is provided by planning for and deploying infrastructure and application redundancy and availability. Each BSS application architecture includes a failover site in geographically dispersed locations. Application databases are replicated in real-time or near real-time depending on the application classification and application's RTO and Recovery Point Objective (RPO).

The BSS System Security Plan (SSP) describes how the system availability controls are implemented, tested, and maintained and includes the CP, DRP, and BIA as appendices. Once the DRP is prepared, we test it as discussed in **Appendix G** and revise as necessary before distributing it to the stakeholders. We include the DRP, along with the CP and the BIA, with the initial A&A package and, as revised, annually thereafter.

A-10 Additional Elements of the Program Management Approach [L.30.2.1]

A-10.1 Personnel Security [H.35]

GSA requires cleared security POCs who will process background investigations and security clearances to be compliant with sensitive government physical and information security requirements. AT&T will provide security expertise with national security checks and appropriate levels to GSA to meet the security requirements in RFP Section G.9.3.7. AT&T accomplishes this through the responsibilities of the Facilities Security Office (FSO) and the information Systems Security Officer (ISSO). The AT&T EIS ISSO will be the Security Point of Contact for GSA.

Process: GSA expects an efficient and accountable process for all security clearances processing. The AT&T process to meet these needs is to identify personnel security requirements; provide oversight and control over personnel assignment; manage personnel readiness including all required security awareness and procedural training; and provide security control oversight via a designated AT&T ISSO.

Our FSO manages suitability and clearance applications for AT&T personnel. The FSO identifies staff required to submit clearance applications, or be granted the required suitability or other clearances required to staff EIS and TO specific needs

The AT&T EIS ISSO follows a documented process to verify specific TO security requirements. AT&T recognizes that personnel will be required to undergo background investigations to access components or system-sensitive information. AT&T process controls preclude individual AT&T staff members from self-select participation in security background investigations for suitability or other clearances.

Agency requests for access will be forwarded to the AT&T FSO, which initiates the background investigation process and coordinates this with the government. Once the background investigation is complete, the AT&T FSO notifies the AT&T employee to complete required security process and awareness training. Once trained, the EIS ISSO is apprised of the individual's status as ready for assignment. The EIS ISSO independently verifies with the AT&T FSO on the suitability or clearance status of the AT&T employee to be granted clearances. Once verified, the AT&T FSO grants access to the cleared, trained, validated employee. From this point, the AT&T FSO tracks training status in a database, and prompts AT&T employees to complete their annual refresher training per GSA/agency requirements.

The EIS ISSO audits for approved access on a quarterly basis, in accordance with the TO security requirements, to confirm only properly credentialed personnel have access to restricted programs, and that all staff security training and awareness is current. The EIS ISSO performs these account verifications throughout the lifecycle of the TO.

AT&T established this process to verify TO security controls are identified, understood, and implemented at system startup and throughout the entire system lifecycle. The

practice of having the AT&T FSO and EIS ISSO perform overlapping security tasks provides checks, balances, and cross-validation. It also provides for

clear separation of duties when assigning least privilege role based access to personnel. The GSA receives a process that is transparent, stringent and protects systems from unauthorized access by inappropriate or unauthorized personnel.

A-10.2 Deliverables and Reports [D; F]

AT&T commits to deliver all work products and contractually required reports such as those listed in RFP F.2.1 Table of Deliverables. We also commit that our deliverables will meet professional standards and the standards set forth in the EIS contract.

The AT&T EIS PM provides GSA a single point of accountability for the quality of AT&T reports and deliverables. The CSO reviews all work products prior to submission to validate compliance with all EIS contractual requirements, including:

- Deliverable content, schedule, and quality standards (F.2)
- EIS packaging and marking requirements (D.1-D.4)
- Contractor Data Interaction Plan (CDIP) requirements (J.2)
- TO Specific Reports and Deliverables

A-11 Summary

To provide GSA and agencies with an efficient and complete project management plan for EIS, we used our experience and institutional knowledge to create effective procedures; establish a responsive, customer-focused CSO organization; and design a BSS that will provide functionality far beyond the RFP mandatory requirements. Our plan thoughtfully addresses transition needs and proposes a schedule that enables an expeditious ATO and transition execution. Moreover, our plan addresses life cycle needs and provides the guiding framework for effectively managing a contract of this scope and scale. Our PMP, as well as our management approach and requisite appendices, will enable and support agency missions and the overall NS2020 vision.



General Services Administration (GSA)

Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

GS00Q17NSD3000
Appendix B — SCRM Plan

APPENDIX B — SCRM PLAN [L.30; L.30.2.2; M.2.2 (1 OF 7); G.6.3]

The primary objective of this Supply Chain Risk Management (SCRM) Plan is to protect and uphold the efficient and secure provisioning of products, services, and materials throughout the usage life cycle through the identification, assessment, and mitigation of threats. This focus fosters a more resilient supply chain through not compromising on the integrity of goods by addressing threats at the early stages of acquisition and providing adequate security. We prioritize efforts to alleviate systemic vulnerabilities and refine strategies to reconstitute the flow of business after disruptions to achieve this goal.

For Enterprise Infrastructure Solutions (EIS), AT&T approaches supply chain risk by sharing procedures and policies and making sure of compliance adherence by our suppliers and vendors.

EIS will benefit from continuous execution of the plan through the AT&T Supply Chain Management Organization and the associated purchasing policies and procedures that are applicable in all stages of the acquisition life cycle. We provide the following benefits:

- Best-in-Class practices regarding product and support quality
- Pricing review and analyses through its “should cost” pricing team
- Application of environmental (sustainability) practices; for example, the reduction of carbon emissions from its suppliers
- TL9000 and ISO28000 certification for the Supply Chain Management Organization

The SCRM Plan is built on the foundation of the AT&T Security Policy and Requirements (ASPR) corporate security policy, as it relates to the protection of AT&T Global Supply Chain (GSC), which governs the life cycle of mission-critical products, services, and materials. The SCRM Plan identifies the AT&T policies and practices that we continuously monitor, track, and update to prevent vulnerabilities, eliminate threats, and minimize risks.

This SCRM Plan describes AT&T adherence to ISO 27001:2013 certified processes and procedures that are in process of being certified ISO 28000:2007. The SCRM Plan also conforms to the National Institute of Standards and Technology Special Publication

(NIST.SP) 800-161, “SCRM Practices for Federal Information Systems and Organizations,” which makes certain of resilience throughout the AT&T GSC. Implementing protective measures and corresponding with the sensitivity, value, and critical nature to the supply chain, the processes and procedures described in this plan serve as guidance that guards against counterfeit, unauthorized or improper use, theft, accidental or unauthorized modification, disclosure, transfer, or destruction of resources.

Supported by the SCRM Plan, the GSC provides direction and leadership for AT&T, which results in the development and implementation of sourcing strategies companywide. The company is responsible for the negotiation of both network and non-network materials and services used within AT&T. GSC provides advice and counsel for international engagements and strengthens the AT&T competitive market position and purchasing power by working with suppliers to reduce expense and maximize the quality and reliability of the products and services purchased by AT&T.

AT&T GSC manages the following corporate functions depicted in **Figure B-1**.

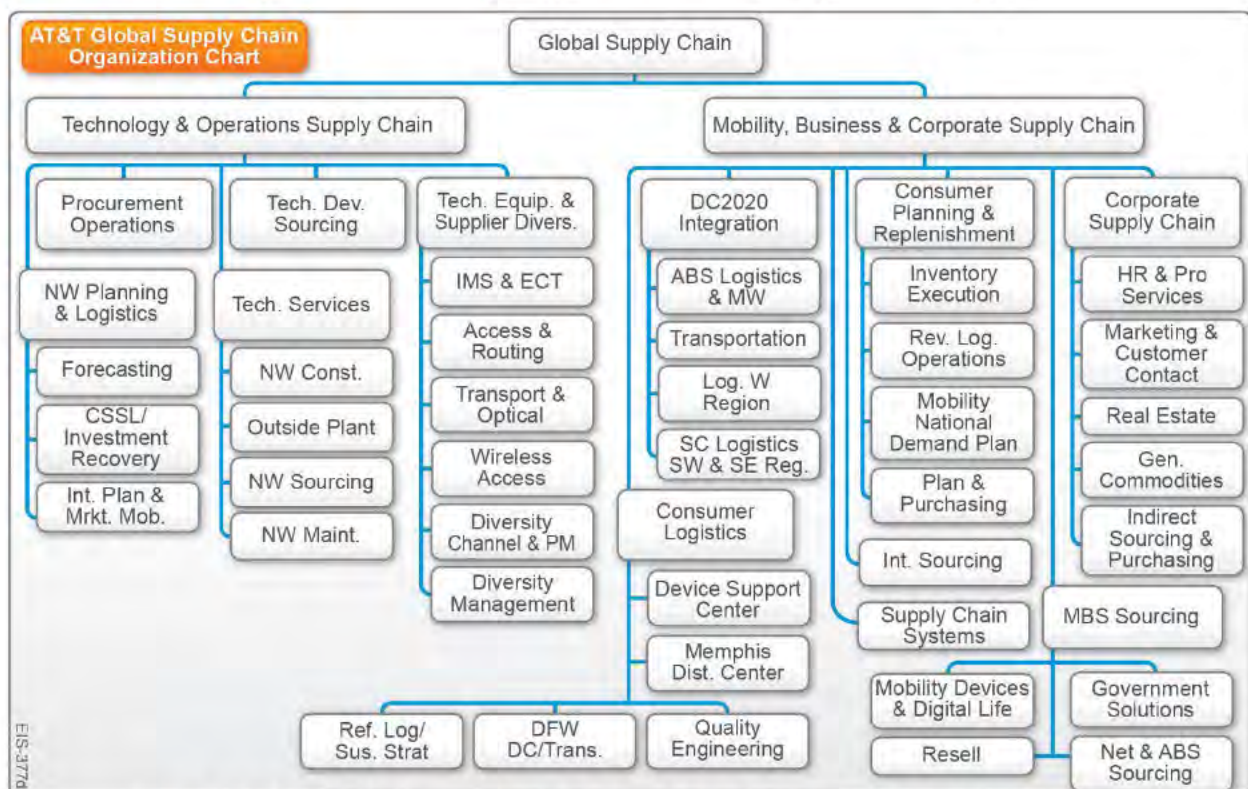


Figure B-1. AT&T Global Supply Chain Organization. AT&T provides the necessary supply chain management, experience and understanding to meet the needs of GSA and agencies.

The SCRM Plan allows for management of controllable and uncontrollable scenarios such as the those described in **Table B-1**. AT&T believes securing the global supply chain is a critical and valuable undertaking that places a premium on Information Technology (IT) security, addresses existing challenges, and enables new opportunities.

Table B-1. AT&T SCRM Plan Benefits. AT&T continually audits and improves upon internal processes in order to evolve with the changing needs of the company, our customers, and ever-evolving supply chain challenges.

Highlights	Benefits
Multi-Sourcing	Reduce exposure to logistics disruptions
Trained and Vetted Employees	Lower risk of compromise
Process and Tool Evolution	Evolve at the pace of technology
Cyber and Physical Security	Inspect and monitor for tampering
Extend Supply Chain Through Sustainment	Ensures Operations and Maintenance (O&M) Maintains System Security
Adherence to Standards (e.g., ISO 27001/ISO 28000)	Validated Processes for Repeatability

B-1 AT&T's Approach to SCRM [L.30.2.2; G.6.3]

The AT&T approach to SCRM is to apply multiple methods of design, implementation, and security to our SCRM tools and purchasing processes with our suppliers. These various approaches are collected in the AT&T supplier agreements and the AT&T operating procedure entitled, "Global Supply Chain Supplier Contracting Policy." The following list describes some of the AT&T SCRM processes that suppliers must adhere to if they will actively pursue a business relationship with the company. Some of the processes include:

1. Requiring all key network and software suppliers to use TL9000 quality standards
2. Continuously monitoring suppliers' products against an established set of key performance metrics, such as failure rate of components, and reviewing the results with suppliers on a quarterly basis.
3. Collaborative interactions are supported by the AT&T Supplier Portal, which is depicted in **Figure B-1-1**.



Figure B-1-1. AT&T Supplier Portal.
AT&T continually monitors and assesses collaborative environments to prevent potential harm.

4. All supplier contracts include an individualized set of inspections, acceptance, and performance testing requirements that are based on the components or services they deliver. These requirements are verified and assessed with lab testing and/or field installation. Test criteria are pre-established and detailed in the Partner Evaluation Criteria in **Figure B-1-2**.

5. Prior to selection as an AT&T supplier, we communicate detailed product evaluation and testing standards to the supplier during the product development phase as described in **Figure B-1-3**. We test new products to meet AT&T operational requirements before they are approved and deployed.

6. AT&T has a formal third-party assessment program developed and performed by our Chief Technology Office (CTO) organization for suppliers. We conduct auditing of cloud-based services for security and quality standards, which are applied prior to a supplier's opportunity to deliver these services to AT&T and its customers.

7. Suppliers' financial viability is assessed in addition to the application of the quality standards necessary to do business with AT&T.

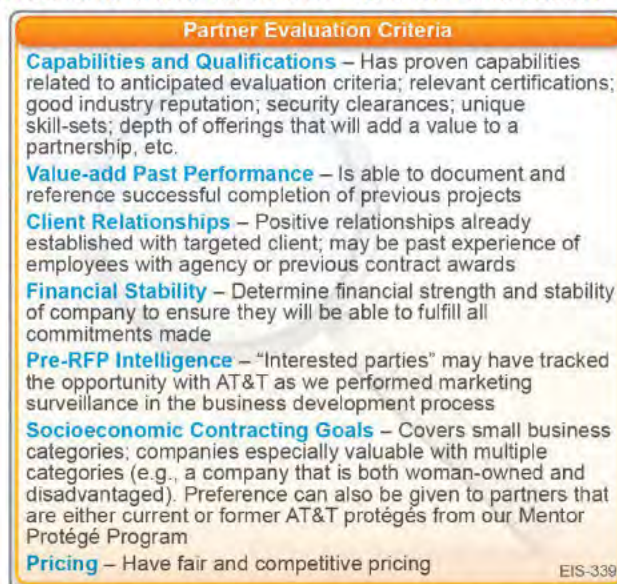


Figure B-1-2. Partner Evaluation Criteria.
AT&T Supplier evaluation makes certain partners are solvent and meet/exceed set AT&T quality standards.

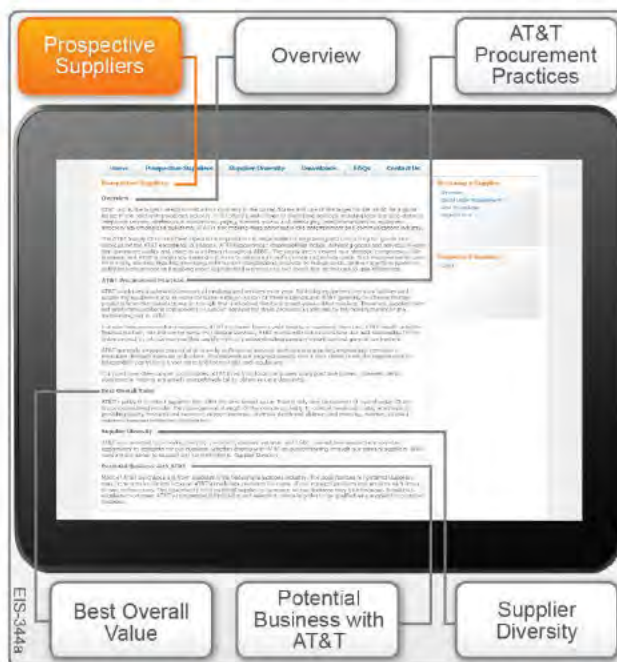


Figure B-1-3. AT&T Prospective Suppliers Website.
AT&T provides Suppliers with information to set expectations for a successful engagement.

8. Regular auditing of suppliers to verify conformance to TL9000 quality standards is performed. If audit exceptions are detected, suppliers are then subjected to root cause analyses as part of corrective action. **Table B-1-1** shows the top five supplier quality metrics that are derived from the TL 9000 handbook, which comprise the AT&T report card. There are numerous measurements captured as part of the AT&T overall report card that is available upon request.
9. AT&T suppliers are required to adhere to AT&T Supplier Information Security Requirements (SISR), which are the codified requirements of the AT&T supplier agreement. The Offshore Oversight Committee, which is governed by the AT&T offshore services supplier contracting policy, conducts detailed reviews of any foreign or offshore products/services to confirm employees and products are not from high-risk countries.

Table B-1-1. AT&T TL9000 Measurements Summary Listing. AT&T holds Suppliers to Quality Standards.

Number	Paragraph	Measurements	Measurement Symbol ¹	Applicability ²	Reported Items (table) ³	Compared or Researched Data
1	5.1	Number of Problem Reports (NPR) Formulas: Table 5.1-2	NPR	H,S,V	5.1-3, 5.1-4, 5.1-5	Compared
2	5.4	On-Time Delivery (OTD) Formulas: Table 5.4-2	OTD	H,S,V	5.4-3	Compared
3	6.1	Service Impact Outage Formulas: Table 6.1-2, 6.1-3	SO	H,S	6.1-4	Compared
4	8.2	Software Problem Reports (SPR) Formulas: Table 8.2-2	SPR	S	8.2-3	Compared
5	9.2	End-Customer Complaint Report Rate Formulas: Table 9.2-2	CCRR	V	9.2-3	Compared

Legend:

¹The symbols used in data reporting (Measurement Symbol)

²The applicability to hardware, software, and/or services (H, S, V), and

³A reference to the AT&T TL9000 measurements table with data reporting details.

B-2 Demonstration of How AT&T's Approach Will Reduce and Mitigate Supply Chain Risks [L.30.2.2; G.6.3]

Sections B-1 and B-3 describe the AT&T process of reducing and mitigating supply chain risks. Our comprehensive methodologies make certain we have suppliers that have been through a rigorous vetting process underpinned by a supplier agreement and continuously monitoring contractual criteria. AT&T develops and implements an effective combination of legal safeguards, situational awareness throughout the global supply chain, proactive defense measures, and product protection instruments with top management awareness of secure information protection. We increase awareness and education among employees and suppliers about the danger of leaks, create unique specific packaging, and inform customers how to spot non-authentic products. We also cooperate closely with all suppliers in our global supply chain. It is crucial to reduce vulnerability to counterfeit products, services, and materials as much as possible, allowing our customers to focus on core mission objectives. AT&T recognizes that supply chain protection is an on-going process that requires continuous attention.

B-3 Management of Supply Chain Risk throughout Each of the Five Supply Chain Phases [L.30.2.2; G.6.3]

Figure B-3-1 visually shows the protection of the supply chain throughout the life cycle. AT&T adds an additional step in front of the five-supply chain phases defined in the RFP. This supplier step requires our vendors to accept AT&T security requirements before even engaging with them in our supply chain and helps to identify specified supporting infrastructure beyond the system boundary where appropriate.

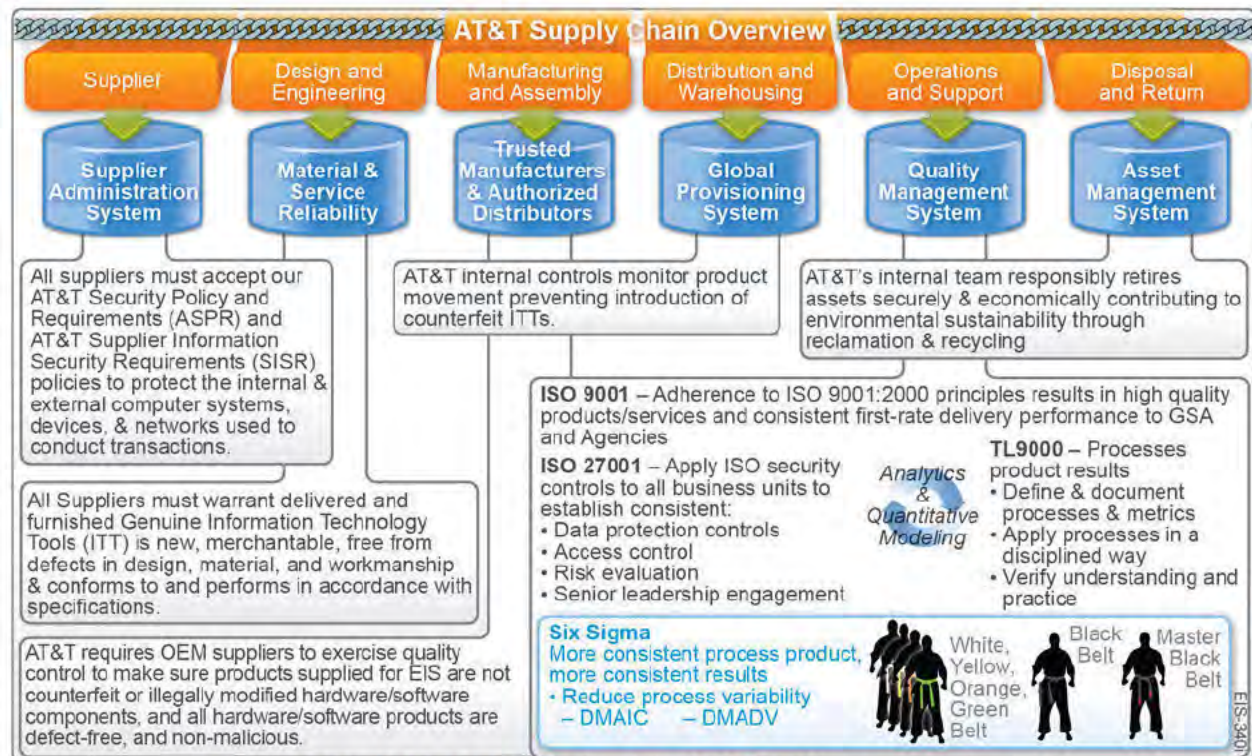


Figure B-3-1. AT&T SCRM Overview. The AT&T SCRM process continuously monitors, tracks, assesses, and mitigates threats to the supply chain.

The following table describes our SCRM Plan as depicted in **Figure B-3-1**. Our approach manages supply chain risk throughout each of the five supply chain phases starting with our suppliers. **Table B-3-1** describes how AT&T will manage risk throughout each of the phases for EIS customers with additional supporting information discussed in **Sections B-3-1** through **B-3-5**.

Table B-3-1. AT&T Five Supply Chain Phases. Threat Mitigation and Reduction through Continuous Assessment.

Supply Chain Phases	AT&T Compliance with Requirements
1. Suppliers	The AT&T supplier sourcing/selection process includes risk assessment in all potential risk areas, such as financial and market stability, sustainability, product and service performance, quality, supplier's ability to comply with AT&T quality assurance (QA), security requirements, and citizenship & sustainability policies, including specified supporting infrastructure beyond the system boundary.
2. Design and Engineering	AT&T identifies and eliminates counterfeit or illegally modified products. We analyze modified products to determine if intent was malicious rather than for profit.
3. Manufacturing and Assembly	Using only proven and trusted manufacturers and authorized distributors who have established agreements and strong relationships with AT&T. AT&T identifies and eliminates counterfeit or illegally modified products. We analyze modified products to determine if intent was malicious rather than for profit.
4. Distribution and Warehousing	Requiring any suppliers whose products or services are manufactured in, shipped from or performed in foreign countries be vetted and approved to meet import-export requirements of our Global Trade Organization and adhere to all foreign trade policies of our Offshore Governance organization.

Supply Chain Phases	AT&T Compliance with Requirements
	Well-established AT&T corporate systems used for procurement of hardware/software from thousands of vendors to support commercial and government customers. These systems automatically feed procurement data to downstream AT&T databases, which we use for managing assets during the subsequent phases (disposal and return). AT&T has specialized staging centers that use internal personnel and outside vendors to provide a secure environment.
5. Operations and Support	We follow the following quality standards and processes in support of the supply chain sustainability: - ISO 9001 and 28000 - Adhere to the principles of ISO 9001:2000 result in delivery of consistent, excellent performance, with high quality products and services, to GSA and agencies. - Third Party Assessment Process (TPAP) Standard corporate program to assess third-party vendors. Assessment categories include, but are not limited to capacity management, IT integration, architecture & design, security, operations, and customer experience.
6. Disposal and Return	The AT&T Asset Management Team manages the return and disposal of equipment by adhering to the component retrieval process outlined in AT&T's internal policy OP123 that covers the retrieval of any AT&T company asset. We track the equipment's final disposition by monitoring UPS shipping numbers and confirming with the receiving party that the asset has arrived at the designated disposal site with any sensitive government information clean/wiped from the gear. As an additional safeguard, we check EIS customer hardware upon arrival at the final disposition location.

B-3.1 Design and Engineering [L.30.2.2(1 of 5); G.6.3(1 of 5)]

This stage is documented and followed per AT&T TL9000 standards and is performed by the AT&T CTO. Our architects qualify and test new designs and products. If the product is supplier based, as part of the product selection process, AT&T CTO and GSC sends out technology surveys, proposal requests, or questionnaires to numerous potentially qualified suppliers.

CTO Lab designers and engineers carefully review technology survey responses against specifications, budgets, and timelines. If an AT&T supplier passes the technology survey process, we will select the supplier's components for product evaluation. We execute Product Evaluation Agreements (PEA) to cover this phase in the AT&T supply chain. We subsequently track CTO Lab product test results. CTO Lab evaluates and tests all products against AT&T specifications and customer requirements. Only after satisfactory testing are these products Approved for Use (AFU). We then codify AFU specifications into AT&T supplier agreements for successive delivery and product acceptance testing prior to installation into AT&T or a customer network. Defective products that are detected during acceptance testing in CTO Lab or Network Operations (engineering) are returned to the supplier for corrective

action and analysis. The supplier must follow the AT&T engineering and supply chain quality assurance process to determine root cause analysis per TL9000 standards and AT&T supplier agreement terms.

B-3.2 Manufacturing and Assembly [L.30.2.2(2 of 5); G.6.3(2 of 5)]

GSC requires all network suppliers to adopt TL9000 quality standards affecting manufacturing and assembly or provide verification that they have an implemented quality control process. We audit AT&T suppliers against the quality control standards, and they must demonstrate compliance to AT&T SISR to protect against security threats, including unauthorized access/intrusion, and exfiltration of sensitive information. The GSC tracks quality metrics and reviews them quarterly with the affected supplier for corrective action and status. Upon delivery, products are tested before installation by AT&T Network Operations to meet AT&T specifications.

B-3.3 Distribution and Warehousing [L.30.2.2(3 of 5); G.6.3(3 of 5)]

We receive and inspect all AT&T supplier products pursuant to AT&T TL9000 policy entitled, "General Procedure Warehouse Operations (WO) Receiving/Receiving Process WO-002, AT&T Services, Inc. Warehouse Operations." We carefully inspect AT&T supplier products against an order for product ID and serial number. Items are given Human Equipment Category Inventory (HECI) codes, barcoded, and secured in a restricted-entry AT&T warehouse. AT&T inventory is processed and tracked under the AT&T Logistics and Inventory Control (LOGIC) system as part of the Oracle Advanced Supply Chain Planning (ASCP) platform.

B-3.4 Operations and Support [L.30.2.2(4 of 5); G.6.3(4 of 5)]

AT&T Asset Management and AT&T Network

Operations track and monitor AT&T network products and software per TL9000 standards. AT&T Operations performs product testing during installation pursuant to

inspection procedures maintained in its Network Equipment-Building System (NEBS) database. If defective products are found, the product is removed and quarantined by placing a red label on the product. During the secure quarantine period, we perform a root cause analysis on the defect. All defective products are returned to supplier for disposition, including replacement or repair as required by AT&T engineering. GSC is

engaged to assess damages and help facilitate the return and replacement of defective components. We further tested all replaced components to confirm they are defect free.

B-3.5 Disposal and Return [L.30.2.2(5 of 5); G.6.3(5 of 5)]:

The AT&T Asset Management Team manages the disposal and return of equipment by adhering to processes outlined in AT&T internal policy, OP123, which covers the retrieval of any company asset. The equipment's final destination is tracked by monitoring UPS shipping numbers and confirming with the receiving party that the asset has arrived at the designated disposal site with any sensitive government information clean/wiped from the equipment.

Identification of Supporting Infrastructure Beyond the System Boundary: AT&T's supplier policies require complete and extensive identification of systems supporting infrastructure, whether within system design boundaries or beyond. Identification of such "outside boundary support" is covered by AT&T supplier agreements and policies such as Global Supply Chain Supplier Contracting Policy, ASPR and SISR as well as warranty requirements and requirements for adherence to stringent quality control standards and processes such as ISO and TL 9000.

B-4 Mandatory SCRM Requirements That Addresses Counterfeit and Illegally Modified Products [L.30.2.2; G.6.3]

Products are carefully inspected and tested prior to being installed into the AT&T network or a customer-managed service network. In all cases, AT&T technicians review each piece of equipment to confirm it is genuine and from the specified supplier prior to being installed and turned up in the network. The instructions and specifications for equipment review are maintained in an AT&T database that contains all approved specifications and installation instructions entitled, "Technology, Planning & Engineering (TP&E) online library (TDocs)." Furthermore, AT&T monitors its networks and service infrastructure on an ongoing basis. If products are counterfeit or illegally modified, we replace them in a timely manner according to AT&T or customer protocols. We label, quarantine, and return defective items to the AT&T supplier. Corrective action, including root cause analysis to determine how counterfeit or illegally modified products were shipped to AT&T, is performed in accordance with TL9000 standards or contractual mandated terms when problems are found.

B-4.1 How AT&T Ensures that Requirements for Genuine Information Technology Tools (ITT) Are Imposed [L.30.2.2(1 of 11); G.6.3(1)]

AT&T suppliers must comply, as a condition of their supplier agreement, to deliver products that pass AT&T acceptance testing. During acceptance testing all software or products are inspected to be genuine and must perform to AT&T specifications set forth in the supplier agreements. As stated in the warranty provisions of the agreements, the supplier must submit a product that is free from viruses, Trojan horse programs, or back door defects. We monitor compliance via AT&T audits of supplier premises and policies under the Audit Rights contractual term. In addition, AT&T regularly audits network suppliers against TL9000 quality standards every two years.

B-4.1.1 AT&T's Reasonable Steps to Ensure Its SCRM Plan Is Performed for ITT in Its Delivered and Installed Configuration [L.30.2.2(1 of 11)(a); G.6.3(1)(a)]

All products delivered by AT&T suppliers must pass an Acceptance Test Plan as specified in the AT&T supplier agreement. We only install products that pass stringent acceptance testing into our network. Procedures for inspection and testing are in the AT&T operations database entitled, "Technology, Planning & Engineering (TP&E) online library (TDocs)."

B-4.1.2 Equipment Reseller Licensing for OEM Equipment and Software [L.30.2.2(1 of 11)(b); G.6.3(1)(b)]

GSC requires all software or Original Equipment Manufacturer (OEM) equipment used by AT&T has appropriate licensing. The software license provisions in AT&T supplier contracts confirm right-to-use or resell the license to AT&T customers.

B-4.1.3 ITT OEM Exercise of Strict Quality Control [L.30.2.2(1 of 11)(c); G.6.3(1)(c)]

Pursuant to AT&T supplier agreement terms and conditions, key AT&T suppliers and ITT OEMs must comply with TL9000 standards and must pass acceptance testing during the installation and inspection process.

B-4.1.4 AT&T's Traceability of Assurance and Evidence of Genuineness of ITT Back to the Licensed Product and Component OEMs [L.30.2.2(1 of 11)(d); G.6.3(1)(d)]

AT&T traces products delivered in its inventory system by HECI code and tracks them by serial number for all managed services customer accounts. AT&T also verifies the full functionality of all products during its installation by AT&T Network Operations.

B-4.2 AT&T's Use of System Security Engineering Processes [L.30.2.2(2 of 11); G.6.3(2)]

The AT&T Chief Security Officer (CSO) defines all security processes under the AT&T ASPR, which is an ISO27001 certified policy. The AT&T SISR policy defines supplier security specifications. We monitor these standards by AT&T CTO functions in Labs, Engineering, and Network Operations. CSO audits and monitors supplier SISR concerns. In addition, AT&T project management monitors all corrective action with affected suppliers. TL9000 procedures kept in CTO, CSO and supply chain handle policies and standards.

B-4.2.1 Protection Against External Threats [L.30.2.2(2 of 11); G.6.3(2)]

AT&T CSO monitors all supplier systems connections against external threats in accordance with AT&T ASPR policy. All identified supplier security issues or events are reported to supplier via AT&T supply chain. When supplier security issues or events are reported, the AT&T GSC works with the CSO to determine corrective action with affected suppliers. In addition, AT&T Network Operations implements corrective action into procedures via its NEBS platform.

B-4.2.2 Protection Against Hardware and Software Vulnerabilities [L.30.2.2(2 of 11); G.6.3(2)]

All AT&T hardware and software suppliers are required to follow SISR specifications in its AT&T supplier agreement. Suppliers are required to perform testing (e.g., Jenkins Protocols and code reviews) to test for vulnerabilities prior to delivery. All software is delivered to AT&T CTO Labs, which perform security and performance testing on supplier equipment and software. AT&T CSO performs audits of supplier components, including software to verify no vulnerabilities exist.



B-4.3 AT&T's Strategy for Implementing SCRM Security Requirements [L.30.2.2(3 of 11); G.6.3(3)]

AT&T has adopted supplier quality programs based on the global telecommunications TL 9000 requirements & measurements and industry leading practices. The AT&T quality program includes reviewing quality metrics with our network suppliers. We review metrics and related supplier performance report cards quarterly with our key network suppliers. Our strategy for SCRM security addresses more than the security controls set forth in NIST SP 800-53 System Acquisition (SA) family including (SA-12). Our approach is firmly based on our acquisition policy and procedures. Our business model is to avoid counterfeit/illegally modified products by using trusted suppliers. Our acquisition process calls for rigorous supplier selection and contract validation. We protect our information and infrastructure from supplier risks, and we apply the same level of care in protecting the government's information and infrastructure from any risk that may originate from AT&T (or our suppliers). AT&T complies with all SCRM security controls cited in NIST 800-53 Rev4. A brief synopsis is provided in **Table B-4.3-1** of the security controls cited in NIST.

Table B-4.3-1. NIST System Acquisition Controls from NIST Special Publication 800-53A.

SA Requirement and Title	NIST 800-53 Rev4 Description	AT&T Response
SA-1 System and Services Acquisition Policy and Procedures	Evaluate System Acquisition Policy and Procedures — roles, processes, management commitment, coordination among organizational entities.	AT&T supply chain policies requires that supplier products and services be acquired only via AT&T general agreements for the procurement of network products, incorporating customer RFP T's and C's, from a network of pre-qualified suppliers. Our Operating Practice No. 6 (OP6) contains GSC policy and operating guidelines for contracting with suppliers. This policy documents the GSC process and requirements for supplier selection, negotiation, execution and management of transactions and making commitments to purchase, lease, rent, license or otherwise acquire ownership of or right to use equipment, products, supplies, development, materials or services from external suppliers on behalf of the AT&T companies. In addition, ASPR/SISR must be accepted by and complied with by all vendors. AT&T SISR is a supplier related document for security and helps protect against security threats. Our stringent supplier qualification process includes risk assessment in all potential risk areas, including financial and market stability, sustainability, product and service performance and quality, and the supplier's ability to comply with AT&T quality assurance, security requirements, and citizenship and sustainability policies. Contracts with our suppliers include acceptance, performance, delivery, warranty, quality assurance, liability, sustainability, infringement and indemnity clauses that specify compliance criteria for material, hardware and software free from potential defects and risks, as well as for economic, environmental and social sustainability.

SA Requirement and Title	NIST 800-53 Rev4 Description	AT&T Response
SA-2 Allocation of Resources	Allocation of Resources — requirements for the information system or service in mission/business process planning	Our standard acquisition process determines, documents, and allocates the funding for the initial information system or service. AT&T has established an information security program, strict policies and has allocated a group of resources to protect the integrity, confidentiality, and availability of company, supplier and customer assets.
SA-4 Acquisition Process	Acquisition Process— procedures addressing the integration of information security requirements, descriptions, and criteria into the acquisition process etc.	Our standard acquisition process incorporates security functional requirements, security strength requirements, security assurance requirements and other security-related requirements. AT&T has established and proven supply chain processes for managing risk for our government customers. We continually audit and improve upon our internal AT&T processes in order to evolve with the changing needs of the government.
SA-12 Supply Chain Protection	Supply Chain Protection — security safeguards employed to protect against supply chain threats to the information system including: ▪ Acquisition Strategies /tools/methods ▪ Supplier Reviews ▪ Diversity of Suppliers ▪ Minimizing Procurement time ▪ Assessments prior to selection & acceptance ▪ Use of All-Source Intelligence ▪ Operations Security ▪ Validate if components are genuine and not altered	We contractually require our suppliers to provide verification of integrity and traceability. We review supplier processes and key development personnel. We implement security safeguards to reduce the probability of supplier attacks on our information systems and infrastructure. Contracts with our suppliers include clauses that govern acceptance, performance, delivery, warranty, quality assurance, liability, sustainability, infringement and indemnity clauses that specify compliance criteria for material, hardware and software free from potential defects and risks, as well as for economic, environmental and social sustainability. We require OEM suppliers to exercise quality control to ensure that counterfeit or illegally modified hardware or software components are not incorporated into the OEM product, and that all hardware and software products are defect-free. We contractually require suppliers to adhere to AT&T comprehensive SISR for any equipment, hardware or software interacting with AT&T or its customers' networks, systems, data, software, applications, etc. Supplier employees who access AT&T or our customers' facilities undergo strict background checks including drug testing and are to be badged or accompanied at all times. We have a diversity of suppliers. Maximum practical opportunity will continually be afforded to Small, Small Disadvantaged, Women-owned, Veteran-owned, Service-Disabled Veteran-Owned, and Historically Underutilized Business Zones (HUBZone) Small Businesses to participate with us as suppliers, contractors, and subcontractor. In 2014, we spent \$16.5 Billion (27%) of our total expenditures with these suppliers.
SA-19 Component Authenticity	Component Authenticity — anti-counterfeit policy and procedures to detect and prevent counterfeit component from entering the information system	All supplier equipment is acquired through AT&T General Agreements for the Procurement of network Equipment (AGAPE). We flow down to our suppliers the requirements for the use of authentic, non-counterfeit, tamper-free components. AT&T agrees to only buy equipment from the OEM or their authorized distributor/reseller. We require OEM suppliers to exercise quality control to ensure that the products they supply to AT&T for our customers are free from counterfeit or illegally modified hardware or software components, and that all hardware and software products are defect-free, and non-malicious. AT&T Secondary Markets Organization has a dedicated team working with a third-party clearinghouse (Telcordia) to identify and eliminate counterfeit or illegally modified product. AT&T has the in-house technical knowhow both within our Network Engineering or

SA Requirement and Title	NIST 800-53 Rev4 Description	AT&T Response
		Operations organizations as well as within our supply chain organization to identify a suspected "counterfeit".

B-4.3.1 Security Controls Described in NIST [L.30.2.2(3 of 11); G.6.3(3)]

AT&T CSO maintains and monitors All NIST security controls pursuant to ASPR procedures. All procedures are reviewed and updated at least bi-annually and are kept on file. GSC communicates security standards to suppliers via supplier agreements. The CSO, supported by AT&T supply chain, helps monitor and audit suppliers for security processes or concerns.

B-4.3.2 Implementation of the Controls Tailored in Scope to the Effort and the Specific Information [L.30.2.2(3 of 11); G.6.3(3)]

Controls tailored for a supplier are handled within AT&T supplier agreement terms and conditions as well as SISR clauses and specification exhibits. CSO reviews all SISR exceptions found via monitoring or supplier audits.

B-4.4 Criticality Analysis (CA) Process Used by AT&T [L.30.2.2(4 of 11); G.6.3(4)]

AT&T performs CA under its Supplier Performance Management Application within the AT&T web-based platform. The Supplier Performance Management Application has predefined critical analysis data points that we capture and track to provide on-going reporting of key supplier quality metrics. **Figure B-4.4-1** depicts the critical analysis framework.

B-4.4.1 Description of AT&T's Supply Chain [L.30.2.2(4 of 11); G.6.3(4)]

AT&T drives the procurement of mission-critical products, services, and materials for customers in all stages of the acquisition life cycle, i.e., from requirements development through products and service design, acquisition, delivery, deployment, and maintenance, to products and services disposition, destruction, decommissioning or retirement. Through engagement with suppliers, all supplier quality and performance data are collected in the AT&T Supplier Performance Management Application.



Figure B-4.4-1. AT&T Critical Analysis.

B-4.4.2 All Critical Hardware and Software Components (and Material Included in Products) [L.30.2.2(4 of 11); G.6.3(4)]

All equipment products must conform to specification for acceptance pursuant to its specific supplier agreement. Results of performance and quality reviews are maintained in AT&T supply chain's [REDACTED] platform and are generally contained in our Supplier Performance Management Application. Furthermore, key network suppliers must conform to TL9000 quality standards.

B-4.4.3 Key Suppliers [L.30.2.2(4 of 11); G.6.3(4)]

AT&T GSC maintains a list of all its key suppliers in the [REDACTED] platform. We monitor all key suppliers for financial viability on an ongoing basis. In addition, performance and quality results are reported and reviewed with AT&T key suppliers. This function resides in AT&T GSC and is recorded in its internal Supplier Performance Management Application.

B-4.4.4 Proof of Company Ownership and Location for Key Suppliers and Component Manufacturers [L.30.2.2(4 of 11); G.6.3(4)]

We financially review key AT&T suppliers on a continuous basis for viability and governance prior to agreement execution. This step is administered via the GSC [REDACTED] and Contracting Policies (OP6). Our suppliers must not only have valid

US Tax IDs, but also must have a current supplier agreement in place to process any order. AT&T will approve foreign locations for products pursuant to our supplier agreements. Ownership or a change in control of a supplier must be pre-approved by AT&T in writing prior to supplier agreement novation or continued agreement performance.

B-4.5 How AT&T Ensures That Products and Components Are Not Repaired and Shipped as New Products and Components to the Government [L.30.2.2(5 of 11); G.6.3(5)]

All deliveries to AT&T undergo two phases of inspection. One is at the AT&T warehouse pursuant to AT&T procedure entitled, “AT&T General Procedure WO Receiving/ Receipting Process WO-002, AT&T Services, Inc.” This procedure requires the warehouse verify the supplier ID and serial number as valid and then secure the asset. Discovered deficiencies require the warehouse to remove, label, and quarantine affected products. We return defective items to supplier for root cause analysis.

The other phase of inspection takes place at installation. The AT&T installing technician or engineer is required to verify and test for performance during installation according to AT&T procedures kept in our [REDACTED] database. The AT&T technician performs a visual inspection and verifies if the product is new by validating that the box has not been previously opened. In addition, the technician matches specifications on installation instructions and procedures, performs functionality testing to check if the product works correctly, and verifies that the equipment does not have indications of damage or tampering. If a defective product is found, it is removed, labelled, quarantined, and returned to supplier for a new replacement and root cause analysis.

AT&T supplier agreements are set up to assess liquidated damages against suppliers if quality or specifications are not met, thereby imposing economic penalties if suppliers do not provide the correct and viable products. In addition, quality audits and metrics are collected within the GSC by working with AT&T Network Operations to track frequencies and categories of deficiencies.

B-4.6 How AT&T Ensures That Supply Channels Are Monitored for Counterfeit Products Throughout the Product Life Cycle to Include Maintenance and Repair [L.30.2.2(6 of 11); G.6.3(6)]

During a network product's life cycle, AT&T Network Operations performs checks on installed equipment via maintenance and inspection walk-throughs at all network sites. Network locations are secured according to ASPR policies with methods such as locked and secure cages for physical tamper protection.

Technicians are required to confirm the product's specification and performance during installation or upgrades. If we discover a problem, we remove the product, label, and quarantine in a timely manner per AT&T supply chain policy entitled, "AT&T General Procedure WO Receiving/Receipting Process WO-002, AT&T Services, Inc.". We notify the supplier who is required to replace the items and perform a root cause analysis in a timely manner. Liquidated damages may be assessed against the affected supplier.

B-4.7 How AT&T's Physical and Logical Delivery Mechanisms Protect Against Unauthorized Access, Exposure of System Components, Information Misuse, Unauthorized Modification, or Redirection [L.30.2.2(7 of 11); G.6.3(7)]

AT&T CSO has established policies, processes, and methods for administering and monitoring against unauthorized access to AT&T facilities and for software with ASPR. We apply the same security controls, as defined by ASPR, to all systems and components used in the procurement of goods and services from our suppliers under SISR in all AT&T supplier contracts. AT&T maintains and updates the procedures bi-annually at a minimum.

AT&T secures against unauthorized access by imposing role-based access controls (RBAC) for both physical and logical access to all system infrastructure components. Suppliers are also required to follow SISR policies, which include personnel background checks required in AT&T supplier agreements for all professional services.

AT&T has implemented firewalls and access control to limit how suppliers access AT&T procurement systems. AT&T imposes strict security control standards that include:

- Monitoring industry resources actively for timely notification of all applicable security alerts that pertain to supplier's information resources and promptly take action to address them.
- Scanning Internet accessible and internal information resources quarterly with industry-standard security vulnerability scanning software to detect un-remediated security vulnerabilities.
- Deploying Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), or Intrusion Detection and Prevention Systems (IDP) in an active mode of operation that monitors all traffic entering and leaving information resources in conjunction with the agreement.
- Using a documented process to remediate security vulnerabilities in the information resources and apply appropriate security patches promptly based on potential risk that a given vulnerability is or will be exploited.
- Assigning security administration responsibilities for configuring host operating systems to specific individuals.
- Verifying that all of supplier's information resources are and remain 'hardened' including, but not limited to, removing or disabling unused networking and other computing services and installing a system firewall, Transmission Control Protocol (TCP) wrappers or similar technology.
- Changing all default account names and/or default passwords.
- Limiting system administrator root, privileged, or super user access to operating systems intended for use by multiple users only to individuals requiring such high-level access in the performance of their jobs.
- Enforcing the rule of least privilege by requiring application, database, network, and system administrators to restrict access by users to only the commands, data and information resources necessary for them to perform authorized functions.
- Verifying that all of supplier's information resources intended for use by multiple users are located in secure physical facilities with access limited and restricted to authorized individuals only.

- Monitoring and recording, for audit purposes, access to the physical facilities containing information resources intended for use by multiple users used in connection with supplier's performance of its obligations under the agreement.
- Using strong encryption for the transfer of in-scope information outside of AT&T-controlled or supplier-controlled networks or when transmitting in-scope Information over any untrusted network. This also applies to in-scope information contained in emails or attachments to emails.
- Requiring strong authentication for any remote access use of nonpublic information resources.

B-4.8 How AT&T's Operational Processes and Disposal Processes Limit Opportunities for Knowledge Exposure, Data Release, or System Compromise [L.30.2.2(8 of 11); G.6.3(8)]

AT&T Supplier Contracting Policy (OP6) requires all suppliers submit to an initial survey and ongoing audits, as needed, to confirm they have adequate security and disposal processes. We handle the disposal of AT&T assets in accordance with AT&T Asset Disposition & Investment Recovery (OP123) policy. Both policies are used and monitored by AT&T Asset Management.

B-4.9 Identification of the Relationship Between AT&T and the Manufacturer [L.30.2.2(9 of 11); G.6.3(9)]

Pursuant to the terms and conditions of all AT&T supplier agreements, suppliers are restricted from identifying a relationship with AT&T unless pre-approved in writing by AT&T. Furthermore, if a product is manufactured for AT&T, the supplier may only use the AT&T logo on the supplier product if it is prior approved by AT&T and within its agreement specification. AT&T carefully inspects each piece of network equipment during installation to make sure it is properly identified and accurately reflects country of origin. Manufacturer product numbers and serial numbers are tracked in AT&T inventory for all customer managed services installations and allow identification of the product source relationship to AT&T (e.g. OEM, Authorized reseller, authorized partner/distributor, or unidentified). This policy is maintained by both AT&T Network Operations and GSC.

B-4.10 AT&T's Expressed Warranty [L.30.2.2(10 of 11); G.6.3(10)]

AT&T customer warranties are written in its customer agreements according to AT&T individual customer requirements. AT&T supplier warranties are written in all its supplier agreements. Software warranties cover customer required conditions such as freedom from viruses, time blocks, back doors and other conditions. If commercial warranties are offered for Commercial Off the Shelf (COTS) products, they will be consistent with 52.246.17. If the commercial warranty is for a period that exceeds one year, the government will receive the additional terms of the commercial warranty.

B-4.11 How AT&T Ensures Independent Verification and Validation of Assurances and Provides Supporting Evidence as Required [L.30.2.2(11 of 11); G.6.3(11)]

AT&T has a formal third-party assessment program developed and performed by our Chief Technology Office (CTO) organization for suppliers. We conduct auditing for security and quality standards, which are applied prior to a supplier's opportunity to deliver supplies or services to AT&T and its customers. These audits include independent verification and validation of assurances. Copies of these audits are available to GSA and agency CO's as requested or required. The requirement for independent verification and validation of assurances is incorporated into our subcontracts whenever the subcontractor provides either personnel, component, or processes identified as a critical component or a part of AT&T's supporting infrastructure

B-5 Inclusion of Information Requirement (G.6.3) in Subcontracts at All Tiers [L.30.2.2; G.6.3]

Pursuant to the terms and conditions of all AT&T supplier agreements, all proprietary and confidential information is restricted from being forwarded to a third party unless AT&T prior approves in writing. All AT&T Suppliers are under Nondisclosure Agreements (NDA) beginning as early as the Request for Proposal (RFP) stage, prior to bidding on products. In addition, we hold subcontractors who are involved with the development or delivery of any information technology, whether acquired as a service or as a supply, to the substance of RFP clause H.37 (including paragraph e) of that clause.

B-6 Identification of All Subcontractors Providing Critical Components or Services and Requirement for Information Necessary to Complete the SCRM Plan [L.30.2.2; G.6.3]

AT&T does not distinguish between suppliers based on the products and services provided. All suppliers must follow AT&T Supplier Agreement terms and conditions. AT&T imposes identical flow-down requirements for all suppliers and their subcontractors. Both are required to meet AT&T requirements regardless of tier or agent status. In addition, all foreign facilities, including all subcontractors, must be pre-approved by AT&T pursuant to the Off Shore Oversight Policy.

B-7 Compliance with NIST SP 800-161 Supply Chain Risk Management Practices [L.30.2.2; G.6.3]

The AT&T overall policy and requirements governing security ASPR serves as a guide and a reference point to conducting business in a secure environment and protecting AT&T assets. ASPR is a set of integrated information security documents. Within ASPR, there are a set of policies and requirements for performing risk management of AT&T services, systems, business units, and suppliers. The ASPR security and risk management policies and requirements comply with NIST SP 800-161 in that they require the following and are updated bi-annually:

1. A tiered approach to implementing the AT&T risk management process. AT&T applies an increasingly stringent risk evaluation process to suppliers with strategic domain suppliers at the top tier with tactical suppliers next. AT&T also applies a tiered Risk Management Framework, shown in **Figure B-7-1**, in how the supply chain places the Enterprise, Business Unit, or Service at risk.



Figure B-7-1. AT&T Risk Framework.

2. AT&T applies an established ISO 270001 Risk Assessment methodology documented in the AT&T ASPR security policy to identify risk based on the unique requirement for the Enterprise as a whole, Business Unit, or Service requirements. The Risk Assessment methodology describes analysis of mission-critical processes, system components, and addresses the vital importance of individual components.

3. The AT&T Risk Assessment process performs an assessment of risk based on the potential severity; impact; and likelihood of the risk occurring at the Enterprise, Business Unit, and Service levels and documented in a Risk Management Assessment document. We periodically assess risks to determine the current security posture.
4. The business leadership at each tier perform an analysis of the risk assessment results to make Enterprise, Business Unit, or Service level risk based decisions to eliminate, accept, mitigate, share, or transfer risk and to implement the necessary controls to mitigate or reduce the risk to the lowest acceptable level. We perform this analysis in accordance with ASPR and ISO guidance.
5. Risks are monitored by business unit leadership at all tiers to periodically re-evaluate the effectiveness of implemented controls used to eliminate or mitigate risk and that tools for monitoring risk are implemented within AT&T Enterprise-Wide continuous monitoring program managed by the AT&T Chief Security Office.

AT&T applies Risk Management as an umbrella concept, which includes Security compliance as a major component. Supply chain management uses a contract with the supplier as a foundation to Risk Management. The key elements of the contract to manage Risk Management includes indemnity, infringement, warranty, financial audit and compliance, insurance, and background check provisions.

B-8 SCRM Plan Updates [L.30.2.2; G.6.3]

The AT&T CSO updates security documents and policies, SISR and ASPR, bi-annually. We review suppliers' compliance against AT&T policies for SCRM during the administration of the supplier agreement and during supplier selection and agreement renewals. As shown in **Figure B-8-1**, our processes are done repeatedly and consistently in order to maintain quality control.

Figure B-8-1. AT&T Continuous Improvement Framework.

B-9 Plan Submittal and Review [G.6.3.1]

AT&T provides this plan with our initial proposal. We will update this plan in response to NIST SCRM guidelines as well as changes driven by lessons learned and industry best practices. We will provide updates on an annual basis to the Contracting Officer (CO) and the Contracting Officer's Representative (COR). Modifications to our SCRM will be done at no additional cost to the government.

In summary, AT&T global supply chain provides GSA and agencies a product that conforms to strict quality and security practices to meet all EIS requirements. Through an emphasis on IT security, new supply opportunities will be enabled, presenting new solutions to old challenges. Along this line, the AT&T GSC will meet and exceed EIS requirements.



General Services Administration (GSA)

Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

GS00Q17NSD3000

Appendix C — Draft BSS Verification Test Plan

APPENDIX C — DRAFT BSS VERIFICATION TEST PLAN]

This section features our proposed Business Support Systems (BSS) Verification Test Plan (BSS Test Plan), compliant with instructions in RFP Section L.30.2.3 and the test methodology specified in RFP Sections E.2.1.1 through E.2.1.5 and supports the management functionality described in RFP Section G. It addresses security testing based on functional requirements shown in RFP Section G.5.6. [REDACTED]

[REDACTED] Our test plan also adheres to RFP Section L.11 security requirements for unclassified information technology resources including personnel and equipment as defined within General Services Acquisition Manual (GSAM) 552.239-71.

Our Business Support Systems (BSS): [REDACTED]

Figure C-1, [REDACTED]

Figure C-1. AT&T Portal and BSS.

Section 1.1.3.4 of this proposal.

[REDACTED]

[REDACTED]

Appendix G

[REDACTED]

Figure C-2.

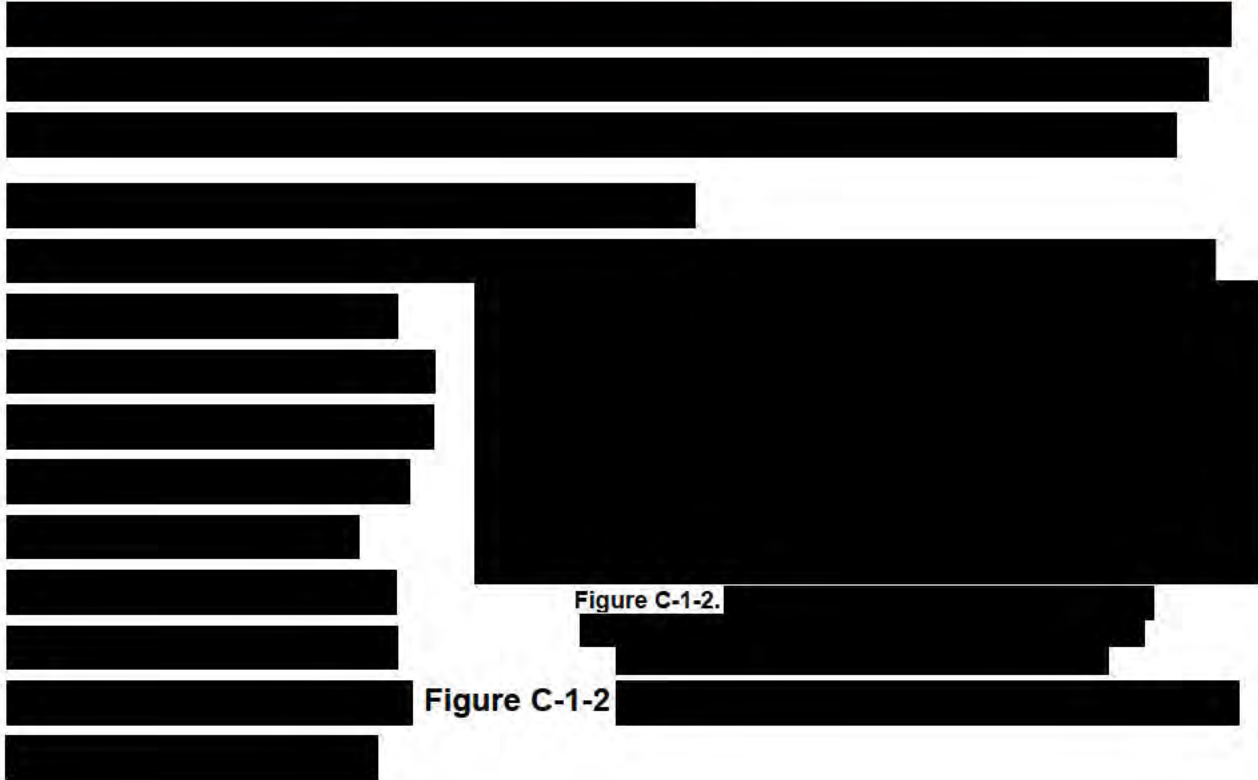


Figure C-2. BSS Verification Test Approach. [Redacted]

C-1 Scope [L.30.2.3; E.2.1.1]



Figure C-1-1. BSS Verification Test Plan Scope. [Redacted]



C-1.1 BSS Testing Verification That All BSS Functional, Regression, Load, and Security Requirements Have Been Successfully Met [L.30.2.3(1); E.2.1.1]

Per GSA's guidance, in RFP Section G.5.1 the BSS Overview,

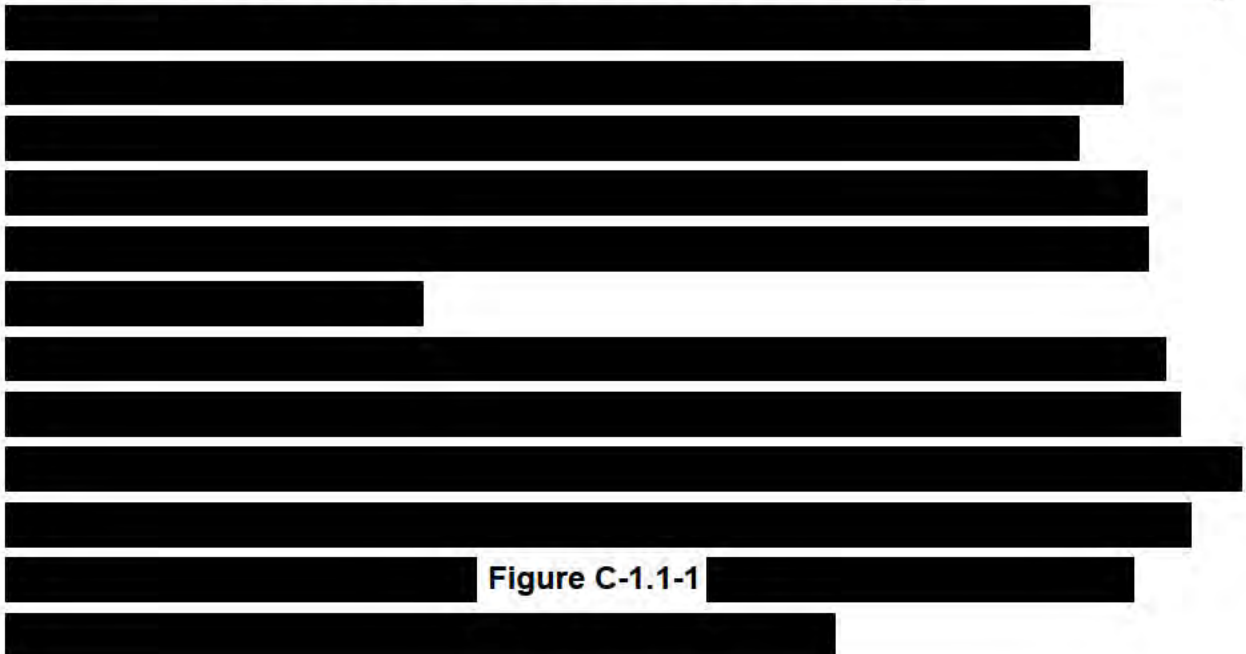




Figure C-1.1-1. AT&T Continuous Delivery Process.



C-1.2 Performance of BSS Testing for All Management and Operation Functions [L.30.2.3(2); E.2.1.1]



C-1.2.1 Ordering [L.30.2.3(2); E.2.1.1]



[REDACTED]

C-1.2.2 Billing [L.30.2.3(2); E.2.1.1]

[REDACTED]

C-1.2.3 Inventory Management [L.30.2.3(2); E.2.1.1]

[REDACTED]

C-1.2.4 Disputes [L.30.2.3(2); E.2.1.1]

[REDACTED]

C-1.2.5 SLA Management [L.30.2.3(2); E.2.1.1]

[REDACTED]

C-1.2.6 Trouble Ticketing [L.30.2.3(2); E.2.1.1]

**C-1.3 Security Testing Based on BSS Security Requirements
[L.30.2.3(3); E.2.1.1]**

In support of A&A and in accordance with guidance from National Institute of Standards and Technology (NIST) SP 800-37, [REDACTED]

Age Group	Percentage
18-24	45%
25-34	55%
35-44	40%
45-54	35%
55-64	25%
65-74	30%
75-84	50%
85-94	55%
95-104	10%
105-114	5%

Upon the start of the BSS Verification Test, [REDACTED]

[REDACTED]

C.1.7 Performance of BSS Verification Testing [E.2.1.1]

Once GSA accepts the BSS Verification Test Plan, we will perform testing on a date accepted [REDACTED]

C-2 BSS Test Scenarios [E.2.1.2]

The BSS Verification Test outlines a series of BSS test scenarios. There are individual test cases under each scenario. GSA provides test data sets with at least two complete data sets for each test case. [REDACTED]

C-2.1 Testing Prerequisites [E.2.1.2.1]

[REDACTED] Our security and functional testing are conducted per the definitions in RFP Section G.5.6, BSS Security Requirements, and RFP Section G.2.3, BSS Final Contract Acceptance.

C-2.2 Test Scenarios [E.2.1.2.2]

Section 3

Figure C-2.2-1 [REDACTED]

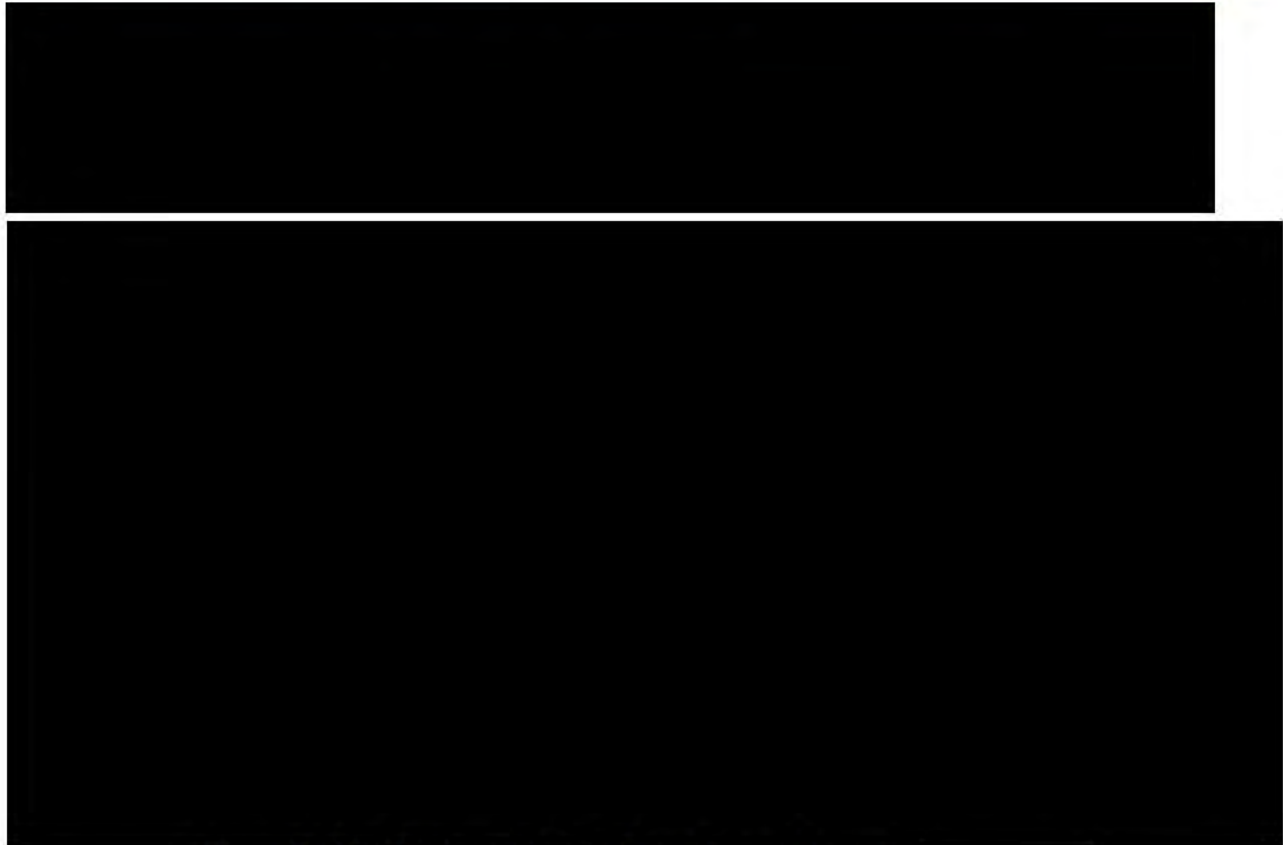


Figure C-2.2-1. BSS Verification Test Execution and Approach.

The BSS Verification Test outlines a series of BSS Test Scenarios. There will be individual test cases under each scenario. GSA will provide test data sets including at least two complete data sets for each test case. Using an approved test plan, schedule, and location, we will perform the BSS Verification Test to meet the acceptance criteria for all test scenarios and related test cases. **Table C-2.2-1** shows a summary of the expected BSS Test Scenarios, which are further detailed in subsequent paragraphs.

Table C-2.2-1. BSS Verification Test. *Our BSS Verification Test Plan drills down to functional details for comprehensive testing.*

Section E Paragraph	Section E Requirement	Appendix C BSS Test Plan Reference	RFP References
E.2.1	Business Support Systems Verification Testing		G.2.3
E.2.1.1	Scope	C-1; C.1.2;	
E.2.1.2	BSS Test Scenarios	C-2	
E.2.1.2.1	Testing Prerequisites	C-2.1	
2.1.2.2	Test Scenarios	C-2.2	
E.2.1.3	BSS Test Cases	C-2.1.2; C-3; C-4	
E.2.1.3.1	BSS-TS01: Direct Data Exchange	C-3; C-3.1	G.5.3.2; J.2.9
E.2.1.3.1.1	BSS-TS01-01:XML over Secure Web Services	C-3; C-3.1.1	G.5.3.2; J.2.9

Section E Paragraph	Section E Requirement	Appendix C BSS Test Plan Reference	RFP References
E.2.1.3.1.2	BSS-TS01-02: PSV over SFTP	C-3; C-3.1.2	G.5.3.2; J.2.9
E.2.1.3.1.3	BSS-TS01-03: Error Handling: XML over Secure Web Services	C-3; C-3.1.3	G.5.3.2; J.2.9
E.2.1.3.1.4	BSS-TS01-04: Error Handling: PSV over SFTP	C-3; C-3.1.4	G.5.3.2; J.2.9
E.2.1.3.2	BSS-TS02: Task Order Data Management	C-3; C-.2	G.3; J.2.3
E.2.1.3.2.1	BSS-TS001: Direct Billing Account Setup	C-3; C-3.2.1	G.3; J.2.2; J.2.3
E.2.1.3.3	BSS-TS03: Role Based Access Control	C-3; C-3.3	J.2.3
E.2.1.3.3.1	BSS-TS03-01: Authorized User Access Verification	C-3; C-3.3.1	J.2.3
E.2.1.3.3.2	BSS-TS03-02: Unauthorized User Access Denial Verification	C-3; C-3.3.2	G.5; J.2.3
E.2.1.3.4	BSS-TS04: Service Ordering	C-3; C-3.4	G.3; J.2.4
E.2.1.3.4.1	BSS-TS04-01: New Order via Web Interface	C-3; C-3.4.1	G.3; G.5.3.1; J.2.4
E.2.1.3.4.2	BSS-TS04-02: New Order via Email	C-3; C-3.4.2	G.3; G.5.3.1; J.2.4
E.2.1.3.4.3	BSS-TS04-03: Disconnect Order	C-3; C-3.4.3	G.3; J.2.4; J.2.10.1.1.4.2
E.2.1.3.4.4	BSS-TS04-04: Feature Addition Order	C-3; C-4.4	G.3; J.2.4; J.2.10.1.1.4.2
E.2.1.3.4.5	BSS-TS04-05: Move Order	C-3; C-3.4.5	G.3; J.2.4; J.2.10.1.1.4.2
E.2.1.3.4.6	BSS-TS04-06: TSP Order	C-3; C-3.4.6	G.3; J.2.4
E.2.1.3.4.7	BSS-TS04-07: Auto-Sold CLINs	C-3; C-3.4.7	G.3; J.2.4
E.2.1.3.4.8	BSS-TS04-08: Task Order Unique CLINs (TUCs)	C-3; C-3.4.8	G.3; J.2.4
E.2.1.3.4.9	Reserved		
E.2.1.3.4.10	BSS-TS04-10: Bulk Orders	C-3; C-4.9	G.3; J.2.4
E.2.1.3.4.11	BSS-TS04-11: Error Checking: Missing Info	C-3; C-3.4.10	G.3; J.2.4
E.2.1.3.4.12	BSS-TS04-12: Error Checking: Invalid Info	C-3; C-3.4.11	G.3; J.2.4
E.2.1.3.5	BSS-TS05: Supplements to In-Progress Orders	C-3; C-3.5	G.3; J.2.4
E.2.1.3.5.1	BSS-TS05-01: Cancel Orders	C-3; C-3.5.1	G.3; J.2.4; J.2.10.1.1.4.3
E.2.1.3.5.2	BSS-TS05-02: Service Feature Change	C-3; C-3.5.2	G.3; J.2.4; J.2.10.1.1.4.3
E.2.1.3.5.3	BSS-TS05-03: Location Change	C-3; C-3.5.3	G.3; J.2.4; J.2.10.1.1.4.3
E.2.1.3.5.4	BSS-TS05-04: Change to Customer Want Date	C-3; C-3.5.4	G.3; J.2.4; J.2.10.1.1.4.3
E.2.1.3.5.5	BSS-TS05-05: Change to Administrative Data	C-3; C-3.5.5	G.3; J.2.4; J.2.10.1.1.4.3
E.2.1.3.6	BSS-TS06: Administrative Change Orders	C-3; C-3.6	G.3; J.2.4
E.2.1.3.6.1	BSS-TS06-01: Administrative Change Order	C-3; C-3.6.1	G.3; J.2.4
E.2.1.3.7	BSS-TS07: Rapid Provisioning & Self-Provisioning Orders	C-3; C-3.7	G.3.5.6; J.2.4.2.4
E.2.1.3.7.1	BSS-TS07-01: Rapid Provisioning Orders	C-3; C-3.7.1	G.3; G.5.3.1; J.2.4

Section E Paragraph	Section E Requirement	Appendix C BSS Test Plan Reference	RFP References
E.2.1.3.7.2	BSS-TS07-02: Self-Provisioning Orders	C-3; C-3.7.2	G.3; G.5.3.2; J.2.4
E.2.1.3.7.3	BSS-TS07-03: Self-Provisioning Orders: Error Checking	C-3; C-3.7.3	G.3; G.5.3.2; J.2.4
E.2.1.3.8	BSS-TS08: Inventory and Billing	C-3; C-3.8	G.4; J.2.5; J.2.6; J.2.7; J.2.10
E.2.1.3.8.1	BSS-TS08-01: Inventory Reconciliation	C-3; C-3.8.1	G.7; J.2.7
E.2.1.3.8.2	BSS-TS08-02: Billing	C-3; C-3.8.2	J.2.5; J.2.10
E.2.1.3.8.3	BSS-TS08-03: Usage Based Billing	C-3; C-3.8.3	G.3; J.2.4
E.2.1.3.8.4	BSS-TS08-04: Billing Adjustments	C-3; C-3.8.4	G.4; J.2.5
E.2.1.3.9	BSS-TS09: Dispute Handling	C-3; C-3.9	G.4.4; J.2.6
E.2.1.3.9.1	BSS-TS09-01: Government Initiated Dispute	C-3; C-3.9.1	J.2.3; J.2.6.3
E.2.1.3.10	BSS-TS10: SLA Management	C-3; C-3.10	G.8; J.2.8
E.2.1.3.10.1	BSS-TS10-01: SLA Reporting	C-3; C-3.10.1	G.3; J.2.4
E.2.1.3.10.2	BSS-TS10-02: SLA Credit Request	C-3; C-3.10.2	G.3; J.2.4; J.2.10.3.1.19
E.2.1.3.11	BSS-TS11: Open-Format Reporting	C-3; C-3.11	J.2
E.2.1.3.11.1	BSS-TS11-01: Open-Format Reporting: Samples	C-3; C-3.11.1	G.4; G.5; J.2.100.3.1.13; J.2.10.3.1.24; J.2.10.3.1.25
E.2.1.3.12	BSS-TS12: Regression Testing	C-3; C-3.12	J.2
E.2.1.3.12.1	BSS-TS101: Regression Testing	C-3; C-3.12.1	G.5.5
E.2.1.3.13	BSS-TS13: Security Testing	C-3; C-3.13	G.5.6
E.2.1.3.13.1	BSS-TS13-01: Security Testing	C-3; C-3.13.1	G.5.6
E.2.1.4	Test Results	C-4, C-4.1 through C-4.7	G; G.5; J.2; J.2.10
E.2.1.5	Deliverables	C-5	F.2.1
E.2.1.5.1	Verification Test Plan for Contactor's BSS	C-5.1	G.5.3.1.3; F.2.1
E.2.1.5.2	Verification Test Results Report for Contractor's BSS	C-5.2	G.5.3.1.3; F.2.1

C-3 BSS Test Cases [E.2.1.3]

Table C-3-1.

Table C-3-1. BSS Test Cases.

AT&T will prepare an agenda for each day in advance and we will obtain concurrence on the agenda with the government's representatives. The agenda will outline which test cases are to be accomplished or revisited in that day's session. AT&T will obtain approval from the government's representatives that a given test scenario and test case has been passed with the first set of test data before testing with the second set of test data. If necessary, we will rerun tests (in part or in whole) until the government's comments are satisfactorily addressed. Uncovered issues will be documented and

[REDACTED]

[REDACTED]

[illegible]

C-3.1 BSS-TS01: Direct Data Exchange [E.2.1.3.1]

Table C-3.1-1. Test Case for Direct Data Exchange – XML Over Secure Web Services.

Test Scenario	BSS-TS01: Direct Data Exchange
Test Case ID	BSS-TS01-01
Test Case Description	XML over Secure Web Services [E.2.1.3.1.1]
Requirements Reference(s)	G.5.3.2; J.2.9
Prerequisites	N/A
Government Input(s)	Properly formatted government data set listed as using XML as the transfer mechanism in RFP Section J.2
Expected Output(s)	Properly formatted AT&T data set that meets the following criteria: - Listed as using SFTP as the transfer mechanism in RFP Section J.2 - Includes data derived from the government input
Acceptance Criteria	- Successful transfer of XML data - Correct technical aspects
Data Set Description	Each government-provided test data set will include: One government data set listed as using SFTP as the transfer mechanism in RFP Section J.2

Table C-3.1-2. Test Case for Direct Data Exchange – PSV Over SFTP.

Test Scenario	BSS-TS01: Direct Data Exchange
Test Case ID	BSS-TS01-02
Test Case Description	PSV over SFTP [E.2.1.3.1.2]
Requirements Reference(s)	G.5.3.2; J.2.9
Prerequisites	N/A
Government Input(s)	Properly formatted government data set listed as using SFTP as the transfer mechanism in RFP Section J.2
Expected Output(s)	Properly formatted AT&T's data set that meets the following criteria: - Listed as using SFTP as the transfer mechanism in RFP Section J.2 - Includes data derived from the government input
Acceptance Criteria	- Successful transfer of PSV data - Correct technical aspects
Data Set Description	Each government-provided test data set will include: One government data set listed as using SFTP as the transfer mechanism in RFP Section J.2

Table C-3.1-3. Test Case for Direct Data Exchange – Error Handling.

Test Scenario	BSS-TS01: Direct Data Exchange
Test Case ID	BSS-TS01-03
Test Case Description	Error Handling: XML over Secure Web Services [E.2.1.3.1.3]
Requirements Reference(s)	G.5.3.2; J.2.9
Prerequisites	N/A
Government Input(s)	Invalid government data set listed as using web services as the transfer mechanism in RFP Section J.2
Expected Output(s)	Notification to AT&T of failed import
Acceptance Criteria	- Evidence of failure notification - No partial import
Data Set Description	Each government-provided test data set will include: - One government data set listed as using web services as the transfer mechanism in RFP Section J.2 - One or more XML formatting errors (e.g., missing delimiters)

Table C-3.1-4. Test Case for Direct Data Exchange – Error Handling.

Test Scenario	BSS-TS01: Direct Data Exchange
Test Case ID	BSS-TS01-04
Test Case Description	Error Handling: PSV over SFTP [E.2.1.3.1.4]
Requirements Reference(s)	G.5.3.2; J.2.9
Prerequisites	N/A
Government Input(s)	Invalid government data set listed as using SFTP as the transfer mechanism in RFP Section J.2
Expected Output(s)	Notification to AT&T of failed import
Acceptance Criteria	- Evidence of failure notification - No partial import
Data Set Description	Each government-provided test data set will include: - One government data set listed as using SFTP as the transfer mechanism in RFP Section J.2 - One or more formatting errors (e.g., missing delimiters)

C-3.2 BSS-TS02: Task Order Data Management [E.2.1.3.2]

Tables C-3.2-1 – C-3.2-2

Table C-3.2-1. Test Case for Task Order Data Management.

Test Scenario	BSS-TS02: Task Order Data Management Setup
Test Case ID	BSS-TS02-01
Test Case Description	Direct Billing Account Setup [E.2.1.3.2.1]
Requirements Reference(s)	G.3; J.2.2; J.2.3
Prerequisites	N/A
Government Input(s)	- Task order controlled data as defined in RFP Section J.2.3 - Task order associated data as defined in RFP Section J.2.3 - System Reference data as defined in RFP Section J.2.3
Expected Output(s)	- Accept System Reference Data - Direct Billed Agency Setup (DBAS) CDRL
Acceptance Criteria	- All required CDRLs as defined in RFP Section J.2.3 - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: - Sample TO controlled data transferred in the form of a sample TO - Sample TO associated data transferred in free format (not previously defined) unless AT&T specifies in our proposal that customer registration is to be submitted via their web interface and that interface collects all of the required data - Sample system reference data transferred using the mechanism specified in RFP Section J.2

C.3.3 BSS-TS03: Role Based Access Control [E.2.1.3.3]

Tables C-3.3-1 – C-3.3-2

Table C-3.3-1. Test Case for Role Based Access Control.

Test Scenario	BSS-TS03: Role Based Access Control
Test Case ID	BSS-TS03-01
Test Case Description	Authorized User Access Verification [E.2.1.3.3.1]
Requirements Reference(s)	G.5; J.2.3
Prerequisites	TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	User attempts to: ▪ Sign into BSS ▪ Access BSS areas to which they are an authorized user ▪ Exercise the full range of functionality (read/write) permitted for their role
Expected Output(s)	User is permitted to: ▪ Access to BSS ▪ Access BSS areas as authorized ▪ Exercise assigned functionality
Acceptance Criteria	▪ Access is granted ▪ No security errors displayed
Data Set Description	Each government-provided test data set will include: ▪ Role to be tested ▪ Functionality to be tested

Table C-3.3-2. Test Case for Role Based Access Control – Unauthorized User Access Denial Verification.

Test Scenario	BSS-TS03: Role Based Access Control
Test Case ID	BSS-TS03-02
Test Case Description	Unauthorized User Access Denial Verification [E.2.1.3.3.2]
Requirements Reference(s)	G.5; J.2.3
Prerequisites	TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	User attempts to: ▪ Sign into BSS ▪ Access BSS areas to which they are not an authorized user ▪ Exercise functionality (read/write) not permitted for their role
Expected Output(s)	User is denied access at the point appropriate the role, area and functionality specified in the test data set: ▪ Access to BSS ▪ Access to specific BSS areas ▪ Access to specific functionality ▪ User is shown security error message
Acceptance Criteria	▪ Access is denied ▪ Appropriate errors are displayed
Data Set Description	Each government-provided test data set will include: ▪ Role to be tested (may be specified as none if the set is intended to show denial of unauthorized users) ▪ Functionality to be tested

C-3.4 BSS-TS04: Service Ordering [E.2.1.3.4]

Tables C-3.4-1 – C-3.4-12 show test cases for RBAC.

Table C-3.4-1. Test Case for Service Ordering – New Order via Web Interface.

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-01
Test Case Description	New Order via Web Interface [E.2.1.3.4.1]
Requirements Reference(s)	G.3; G.5.3.1; J.2.4
Prerequisites	TO controlled, TO associated, and System Reference data loaded into AT&T's BSS
Government Input(s)	Service Order (SO) with all required data elements as described in RFP Section J.2.10.2.1.15
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) - Service Order Confirmation (SOC) - Firm Order Commitment Notice (FOCN) - Service Order Completion Notification (SOCN)
Acceptance Criteria	- All required CDRLs as defined in RFP Section J.2.4 - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: - A complete SO for one or more services listed in RFP Section C.2 of the contract - SO to be entered into AT&T's BSS via our web interface as described in RFP Section G.5.3.1

Table C-3.4-2. Test Case for Service Ordering – New Order via Email.

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-02
Test Case Description	New Order via Email [E.2.1.3.4.2]
Requirements Reference(s)	G.3; G.5.3.1; J.2.4
Prerequisites	TO controlled, TO associated, and System Reference data loaded into AT&T's BSS
Government Input(s)	Service Order (SO) with all required data elements as described in RFP Section J.2.10.2.1.15
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) - Service Order Confirmation (SOC) - Firm Order Commitment Notice (FOCN) - Service Order Completion Notification (SOCN)
Acceptance Criteria	- All required CDRLs as defined in RFP Section J.2.4 - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: - A complete SO for one or more services listed in RFP Section C.2 of the contract - SO submitted via a means listed in RFP Section J.2.4 other than AT&T's web interface

Table C-3.4-3. Test Case for Service Ordering – Disconnect Order.

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-03
Test Case Description	Disconnect Order [E.2.1.3.4.3]
Requirements Reference(s)	G.3; J.2.4; J.2.10.1.1.4.2
Prerequisites	TO controlled, TO associated, and System Reference data loaded into AT&T's BSS. Previously provisioned circuit or service element entered into AT&T's BSS
Government Input(s)	Service Order (SO) with all required data elements as described in RFP Section J.2.4 for the disconnect of: ▪ A circuit or service element (CLIN) ▪ A feature of a circuit or service element
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: ▪ Service Order Acknowledgment (SOA) ▪ Service Order Confirmation (SOC) ▪ Firm Order Commitment Notice (FOCN) if required based on the requirements described in RFP Section J.2.4 ▪ Service Order Completion Notification (SOCN)
Acceptance Criteria	▪ All required CDRLs ▪ Accurate data based on inputs ▪ Correct technical aspects
Data Set Description	Each government-provided test data set will include: ▪ A complete SO for the disconnect of a circuit or service element or a feature of a circuit or service element as described in RFP Sections G.3 and J.2.10.1.1.4.2

Table C-3.4-4. Test Case for Service Ordering – Feature Addition Order.

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-04
Test Case Description	Feature Addition Order [E.2.1.3.4.4]
Requirements Reference(s)	G.3; J.2.4; J.2.10.1.1.4.2
Prerequisites	▪ TO controlled, TO associated, and System Reference data loaded into AT&T's BSS ▪ Previously provisioned circuit or service element entered into AT&T's BSS
Government Input(s)	Service Order (SO) with all required data elements as described in RFP Section J.2.4 for the addition of a feature to a circuit or service element
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: ▪ Service Order Acknowledgment (SOA) ▪ Service Order Confirmation (SOC) ▪ Firm Order Commitment Notice (FOCN) ▪ Service Order Completion Notification (SOCN)
Acceptance Criteria	▪ All required CDRLs ▪ Accurate data based on inputs ▪ Correct technical aspects
Data Set Description	Each government-provided test data set will include: ▪ A complete SO for the addition of a feature to a circuit or service element as described in RFP Sections G.3 and J.2.10.1.1.4.2

Table C-3.4-5. Test Case for Service Ordering – Move Order.

Test Case ID	BSS-TS04-05
Test Case Description	Move Order [E.2.1.3.4.5]
Requirements Reference(s)	G.3; J.2.4; J.2.10.1.1.4.2

Test Case ID	BSS-TS04-05
Test Case Description	Move Order [E.2.1.3.4.5]
Prerequisites	- TO controlled, TO associated, and system reference data loaded into AT&T's BSS - Previously provisioned circuit or service element entered into AT&T's BSS
Government Input(s)	- Two Service Orders (SOs) that combine to specify the move of a circuit or service element with all required data elements as described in RFP Section J.2.4 - One SO for the disconnect of the circuit or service element at the old location - Second SO for the installation of the identical circuit or service element at the new location
Expected Output(s)	- Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) - Service Order Confirmation (SOC) - Firm Order Commitment Notice (FOCN) - Service Order Completion Notification (SOCN)
Acceptance Criteria	- All required CDRLs - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: - A pair of complete SOs for the move of a circuit or service element from one valid location to another as described in RFP Sections G.3 and J.2.10.1.1.4.2 - SO for the disconnect from the old location - SO for the installation of the identical service at the new location

Table C-3.4-6. Test Case for Service Ordering – TSP Order.

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-06
Test Case Description	TSP Order [E.2.1.3.4.6]
Requirements Reference(s)	G.3; J.2.4
Prerequisites	TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	Service Order (SO) requesting TSP with all required data elements as described in RFP Section J.2.4
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) - Service Order Confirmation (SOC) - Firm Order Commitment Notice (FOCN) - Service Order Completion Notification (SOCN)
Acceptance Criteria	- All required CDRLs as defined in RFP Section J.2.4 - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: A complete SO with a TSP code for one or more services listed in RFP Section C.2 of the contract

Table C-3.4-7. Test Case for Service Ordering-Auto Sold CLINS.

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-07
Test Case Description	Auto-Sold CLINS [E.2.1.3.4.7]
Requirements Reference(s)	G.3; J.2.4
Prerequisites	TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	Service Order (SO) that includes CLINS with associated Auto-Sold CLINS and contains all required data elements as described in RFP Section J.2.4
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) - Service Order Confirmation (SOC) - Firm Order Commitment Notice (FOCN) - Service Order Completion Notification (SOCN)
Acceptance Criteria	- All required CDRLs as defined in RFP Section J.2.4 - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: A complete SO that includes Auto-Sold CLINS for one or more services listed in RFP Section C.2 of the contract

Table C-3.4-8. Test Case for Service Ordering – Task Order Unique CLINS (TUCs).

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-08
Test Case Description	Task Order Unique CLINS (TUCs) [E.2.1.3.4.8]
Requirements Reference(s)	G.3; J.2.4
Prerequisites	- TO setup data loaded into AT&T's BSS - TO Data defines one or more TUCs - Account Management data loaded into AT&T's BSS
Government Input(s)	Service Order (SO) containing Task Order Unique CLINS (TUCs) and all required data elements as described in RFP Section J.2.4
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) - Service Order Confirmation (SOC) - Firm Order Commitment Notice (FOCN) - Service Order Completion Notification (SOCN)
Acceptance Criteria	- All required CDRLs as defined in RFP Section J.2.4 - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: A complete SO containing TUC for one or more services listed in RFP Section C.2 of the contract

Table C-3.4-9

Table C-3.4-9. Test Case for Service Ordering – Bulk Orders.

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-10
Test Case Description	Bulk Orders [E.2.1.3.4.10]
Requirements Reference(s)	G.3; J.2.4

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-10
Test Case Description	Bulk Orders [E.2.1.3.4.10]
Prerequisites	TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	Bulk Service Order (SO) with all required data elements as described in RFP Section J.2.4
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) - Service Order Confirmation (SOC) - Firm Order Commitment Notice (FOCN) - Service Order Completion Notification (SOCN)
Acceptance Criteria	- All required CDRLs as defined in RFP Section J.2.4 - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: - A SO including at least 20 line items for services listed in RFP Section C.2 of the contract - SO data provided via a delimited text file or MS Excel file

Table C-3.4-10. Test Case for Service Ordering – Error Checking, Missing Information.

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-11
Test Case Description	Error Checking: Missing Information [E.2.1.3.4.11]
Requirements Reference(s)	G.3; J.2.4
Prerequisites	TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	Service Order (SO) missing one or more required data elements as described in RFP Section J.2.4
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) - Service Order Rejection Notice (SORN)
Acceptance Criteria	- All required CDRLs - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: SO missing one or more required data elements for one or more services listed in RFP Section C.2 of the contract

Table C-3.4-11. Test Case for Service Ordering – Error Checking Invalid Info.

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-12
Test Case Description	Error Checking: Invalid Info [E.2.1.3.4.12]
Requirements Reference(s)	G.3; J.2.4
Prerequisites	TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	Service Order (SO) with one or more invalid data elements as described in RFP Section J.2.4
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) - Service Order Rejection Notice (SORN)

Test Scenario	BSS-TS04: Service Ordering
Test Case ID	BSS-TS04-12
Test Case Description	Error Checking: Invalid Info [E.2.1.3.4.12]
Acceptance Criteria	- All required CDRLs - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: - SO orders with one or more invalid data information for one or more services listed in RFP Section C.2 of the contract - Invalid data will include improperly formatted data or data that is inconsistent with the TO or Account Management data

C-3.5 BSS-TS05: Supplements to In-Progress Orders [E.2.1.3.5]

Tables C-3.5-1 – C-3.5-5

Table C-3.5-1. Test Case for Supplements to In-Progress Orders – Cancel Orders.

Test Scenario	BSS-TS05: Supplements to In-Progress Orders
Test Case ID	BSS-TS05-01
Test Case Description	Cancel Orders [E.2.1.3.5.1]
Requirements Reference(s)	G.3; J.2.4; J.2.10.1.1.4.3
Prerequisites	TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	- Service Order (SO) with all required data elements as described in RFP Section J.2.4 - Service Order (SO) for a cancellation of the previous order with all required data elements as described in RFP Section J.2.4 issued prior to completion of the previous order
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) - Updates to Service Order Confirmation (SOC) if required - Updates to Firm Order Commitment Notice (FOCN) if required - Service Order Completion Notification (SOCN)
Acceptance Criteria	- All required CDRLs - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: - A complete SO for one or more services listed in RFP Section C.2 of the contract - A second SO canceling the first Service Order as defined in RFP Section J.2.10.1.1.4.3 - The Cancel Order may be issued before or after the deadline described in RFP Section G.3

Table C-3.5-2. Test Case for Supplements to In Progress Orders – Service Feature Change.

Test Scenario	BSS-TS05: Supplements to In-Progress Orders
Test Case ID	BSS-TS05-02
Test Case Description	Service Feature Change [E.2.1.3.5.2]
Requirements Reference(s)	G.3; J.2.4; J.2.10.1.1.4.3
Prerequisites	TO controlled, TO associated, and system reference data loaded into AT&T's BSS

Test Scenario	BSS-TS05: Supplements to In-Progress Orders
Test Case ID	BSS-TS05-02
Test Case Description	Service Feature Change [E.2.1.3.5.2]
Government Input(s)	- Service Order (SO) with all required data elements as described in RFP Section J.2.4 - Service Order (SO) for a service feature change to the previous order with all required data elements as described in RFP Section J.2.4 issued prior to completion to previous order
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) - Updates to Service Order Confirmation (SOC) if required - Updates to Firm Order Commitment Notice (FOCN) if required - Service Order Completion Notification (SOCN)
Acceptance Criteria	- All required CDRLs - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: - A complete SO for one or more services listed in RFP Section C.2 of the contract - A second SO describing a service feature change to the first Service Order as defined in RFP Section J.2.10.1.1.4.3

Table C-3.5-3. Test Case for Supplements to in Progress Orders Location Change.

Test Scenario	BSS-TS05: Supplements to In-Progress Orders
Test Case ID	BSS-TS05-03
Test Case Description	Location Change [E.2.1.3.5.3]
Requirements Reference(s)	G.3; J.2.4; J.2.10.1.1.4.3
Prerequisites	TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	- Service Order (SO) with all required data elements as described in RFP Section J.2.4 - Service Order (SO) for a location change to the previous order with all required data elements as described in RFP Section J.2.4 issued prior to completion to previous order
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) - Updates to Service Order Confirmation (SOC) if required - Updates to Firm Order Commitment Notice (FOCN) if required - Service Order Completion Notification (SOCN)
Acceptance Criteria	- All required CDRLs - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: - A complete SO for one or more services listed in RFP Section C.2 of the contract - A second SO describing a location change to the first Service Order as defined in RFP Section J.2.10.1.1.4.3

Table C-3.5-4. Test Case for Supplements to In Progress Orders – Change to Customer Want Date.

Test Scenario	BSS-TS05: Supplements to In-Progress Orders
Test Case ID	BSS-TS05-04
Test Case Description	Change to Customer Want Date [E.2.1.3.5.4]
Requirements Reference(s)	▪ G.3; J.2.4; J.2.10.1.1.4.3
Prerequisites	▪ TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	▪ Service Order (SO) with all required data elements as described in RFP Section J.2.4 ▪ Service Order (SO) for a change to the Customer Want Date for the previous order with all required data elements as described in RFP Section J.2.4 issued prior to completion of the previous order
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: ▪ Service Order Acknowledgment (SOA) ▪ Updates to Service Order Confirmation (SOC) if required ▪ Updates to Firm Order Commitment Notice (FOCN) if required ▪ Service Order Completion Notification (SOCN)
Acceptance Criteria	▪ All required CDRLs ▪ Accurate data based on inputs ▪ Correct technical aspects
Data Set Description	Each government-provided test data set will include: ▪ A complete SO for one or more services listed in RFP Section C.2 of the contract ▪ A second SO describing a change to the Customer Want Date for the first Service Order as defined in RFP Section J.2.10.1.1.4.3 ▪ The Customer Want Date Change Order may be issued before or after the deadline described in RFP Section G.3

Table C-3.5-5. Test Case for Supplements to In Progress Orders – Change to Administrative Data.

Test Scenario	BSS-TS05: Supplements to In-Progress Orders
Test Case ID	BSS-TS05-05
Test Case Description	Change to Administrative Data [E.2.1.3.5.5]
Requirements Reference(s)	▪ G.3; J.2.4; J.2.10.1.1.4.3
Prerequisites	▪ TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	▪ Service Order (SO) with all required data elements as described in RFP Section J.2.4 ▪ Service Order (SO) for a change to the administrative data for the previous order with all required data elements as described in RFP Section J.2.4 issued prior to completion of the previous order
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: ▪ Service Order Acknowledgment (SOA) ▪ Updates to Service Order Confirmation (SOC) if required ▪ Updates to Firm Order Commitment Notice (FOCN) if required ▪ Service Order Completion Notification (SOCN)
Acceptance Criteria	▪ All required CDRLs ▪ Accurate data based on inputs ▪ Correct technical aspects
Data Set Description	Each government-provided test data set will include: ▪ A complete SO for one or more services listed in RFP Section C.2 of the contract ▪ A second SO describing a change to the administrative data for the first Service Order as defined in RFP Section J.2.10.1.1.4.3

C-3.6 BSS-TS06: Administrative Change Orders [E.2.1.3.6]

Table C-3.6-1

Table C-3.6-1. Test Case for Administrative Change Order – Administrative Change Order.

Test Scenario	BSS-TS06: Administrative Change Order
Test Case ID	BSS-TS06-01
Test Case Description	Administrative Change Order [E.2.1.3.6.1]
Requirements Reference(s)	G.3; J.2.4; G.5
Prerequisites	- TO controlled, TO associated, and system reference data loaded into AT&T's BSS - One or more previously provisioned orders
Government Input(s)	Administrative Change Order that specifies a change to the administrative data associated with a previously provisioned service as described in RFP Section G.3
Expected Output(s)	- Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Administrative Change (SOAC)
Acceptance Criteria	- All required CDRLs - Accurate data based on inputs - Correct technical aspects
Data Set Description	- Each government-provided test data set will include: - A complete administrative change order for a change to the administrative data for a previously provisioned service as described in RFP Section G.3

C-3.7 BSS-TS07: Rapid Provisioning & Self-Provisioning Orders [E.2.1.3.7]

We accept and execute test cases for the test scenarios in RFP Section E.2.1.2.2.

Tables C-3.7-1 – C-3.7-3 show the test cases for Rapid Provisioning and Self-Provisioning Orders.

Table C-3.7-1. Rapid Provisioning & Self-Provisioning Orders – Rapid Provisioning Orders. GSA and agencies receive all required CDRLs from our fully tested and verified Rapid Provisioning Orders processes.

Test Scenario	BSS-TS07: Rapid Provisioning & Self-Provisioning Orders
Test Case ID	BSS-TS07-01
Test Case Description	Rapid Provisioning Orders [E.2.1.3.7.1]
Requirements Reference(s)	G.3; G.5.3.1; J.2.4
Prerequisites	TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	Service Order (SO) for one or more services subject to rapid provisioning as defined in RFP Section G.3 with all required data elements as described in RFP Section J.2.4

Test Scenario	BSS-TS07: Rapid Provisioning & Self-Provisioning Orders
Test Case ID	BSS-TS07-01
Test Case Description	Rapid Provisioning Orders [E.2.1.3.7.1]
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) if provisioning requires more than 24 hours - Service Order Completion Notification (SOCN)
Acceptance Criteria	- All required CDRLs as defined in RFP Section J.2.4 - Accurate data based on inputs - Correct technical aspects
Data Set Description	- Each government-provided test data set will include: - A complete SO for one or more services subject to rapid provisioning as defined in RFP Section G.3

Table C-3.7-2. Rapid Provisioning and Self-Provisioning Orders – Self-Provisioning Orders. GSA and agencies receive all required CDRLs from our fully tested and verified Self-Provisioning Orders processes.

Test Scenario	BSS-TS07: Rapid Provisioning & Self-Provisioning Orders
Test Case ID	BSS-TS07-02
Test Case Description	Self-Provisioning Orders [E.2.1.3.7.2]
Requirements Reference(s)	G.3; G.5.3.2; J.2.4
Prerequisites	TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	Service Order (SO) with all required data elements as described in RFP Section J.2.4 for one or more services that are: - Subject to rapid provisioning as defined in RFP Section G.3 - Available for self-provisioning as defined in RFP Sections G.3 and C.2
Expected Output(s)	Service Order notification CDRLs as defined in RFP Section J.2.4: - Service Order Acknowledgment (SOA) if provisioning requires more than 24 hours - Service Order Completion Notification (SOCN)
Acceptance Criteria	- All required CDRLs as defined in RFP Section J.2.4 - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: Service Order (SO) with all required data elements as described in RFP Section J.2.4 for one or more services that are subject to rapid provisioning as defined in RFP Section G.3 and that are available for self-provisioning as defined in RFP Sections G.3 and C.2

Table C-3.7-3. Rapid Provisioning & Self-Provisioning Orders – Self-Provisioning Orders: Error Checking. GSA and agencies receive all required CDRLs from our fully tested and verified Self-Provisioning Orders: Error Checking processes.

Test Scenario	BSS-TS07: Rapid Provisioning & Self-Provisioning Orders
Test Case ID	BSS-TS07-03
Test Case Description	Self-Provisioning Orders: Error Checking [E.2.1.3.7.3]
Requirements Reference(s)	G.3; G.5.3.2; J.2.4

Test Scenario	BSS-TS07: Rapid Provisioning & Self-Provisioning Orders
Test Case ID	BSS-TS07-03
Test Case Description	Self-Provisioning Orders: Error Checking [E.2.1.3.7.3]
Prerequisites	TO controlled, TO associated, and system reference data loaded into AT&T's BSS
Government Input(s)	- Service Order (SO) for one or more services subject to rapid provisioning as defined in RFP Section G.3 and available for self-provisioning - Populated via AT&T's Portal with one or more missing or invalid data elements as described in RFP Section J.2.4
Expected Output(s)	- Service Order notification CDRLs as defined in RFP Section J.2.4 - Service Order Rejection Notice (SORN) - User is shown error message indicating failure
Acceptance Criteria	- All required CDRLs as defined in Section RFP J.2.4 - Accurate data based on inputs - Correct technical aspects - Appropriate errors are displayed
Data Set Description	Each government-provided test data set will include: - Service Order (SO) with all required data elements as described in RFP Section J.2.4 for one or more services that are subject to rapid provisioning as defined in RFP Sections G.3 and C.2 - SO to be provided via AT&T's Portal

C-3.8 BSS-TS08: Inventory and Billing [E.2.1.3.8]

Tables C-3.8-1 – C-3.8-4

Table C-3.8-1. Inventory and Billing – Self-Provisioning Orders – Inventory Reconciliation.

Test Scenario	BSS-TS08: Inventory and Billing
Test Case ID	BSS-TS08-01
Test Case Description	Inventory Reconciliation [E.2.1.3.8.1]
Requirements Reference(s)	G.7; J.2.7
Prerequisites	- TO controlled, TO associated, and system reference data loaded into AT&T's BSS - One or more previously provisioned orders
Government Input(s)	N/A
Expected Output(s)	Inventory Reconciliation (IR) CDRLs as described in RFP Section J.2.7
Acceptance Criteria	- All required CDRLs - Accurate data based on inputs - Correct technical aspects
Data Set Description	N/A, see Prerequisites

Table C-3.8-2. Inventory and Billing – Self-Provisioning Orders – Billing.

Test Scenario	BSS-TS08: Inventory and Billing
Test Case ID	BSS-TS08-02
Test Case Description	Billing [E.2.1.3.8.2]
Requirements Reference(s)	J.2.5; J.2.10

Test Scenario	BSS-TS08: Inventory and Billing
Test Case ID	BSS-TS08-02
Test Case Description	Billing [E.2.1.3.8.2]
Prerequisites	- TO controlled, TO associated, and system reference data loaded into AT&T's BSS - One or more previously provisioned orders
Government Input(s)	N/A
Expected Output(s)	Billing CDRLs as defined in RFP Section J.2.4: - Billing Invoice (BI) - Tax Detail Report (TAX) - Associated Government Fee Detailed (AGFD) - AGF EFT Report (ATR)
Acceptance Criteria	- All required CDRLs - Accurate data based on inputs - Correct technical aspects - CDRLs are internally consistent - Complies with calculation rules
Data Set Description	N/A, see Prerequisites

Table C-3.8-3. Inventory and Billing – Self-Provisioning Orders – Usage Based Billing.

Test Scenario	BSS-TS08: Inventory and Billing
Test Case ID	BSS-TS08-03
Test Case Description	Usage Based Billing [E.2.1.3.8.3]
Requirements Reference(s)	G.3; J.2.5
Prerequisites	- TO controlled, TO associated, and system reference data loaded into AT&T's BSS - One or more previously usage based provisioned orders
Government Input(s)	Sample usage data for one or more Unique Billing Identifiers (UBI) based on Usage Based CLIN(s)
Expected Output(s)	Billing CDRLs as defined in RFP Section J.2.5: - Billing Invoice (BI) - Tax Detail Report (TAX) - Associated Government Fee Detailed (AGFD) - AGF EFT Report (ATR)
Acceptance Criteria	- All required CDRLs - Accurate data based on inputs - Correct technical aspects - CDRLs are internally consistent - Complies with calculation rules
Data Set Description	- Each government-provided test data set will include: - Sample usage data for one or more UBI based on Usage Based CLIN(s) - See also Prerequisites

Table C-3.8-4. Inventory and Billing – Self-Provisioning Orders – Billing Adjustments.

Test Scenario	BSS-TS08: Inventory and Billing
Test Case ID	BSS-TS08-04
Test Case Description	Billing Adjustments [E.2.1.3.8.4]
Requirements Reference(s)	G.4; J.2.5

Test Scenario	BSS-TS08: Inventory and Billing
Test Case ID	BSS-TS08-04
Test Case Description	Billing Adjustments [E.2.1.3.8.4]
Prerequisites	- TO controlled, TO associated, and System Reference data loaded into AT&T's BSS - One or more previously provisioned orders - At least one previously submitted Billing Invoice (BI)
Government Input(s)	Sample adjustment request to change or modify a billing line item
Expected Output(s)	Billing Adjustment (BA) as defined in RFP Section J.2.5: Reflects requested adjustment
Acceptance Criteria	- All required CDRLs - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: Sample adjustment request to change or modify a billing line item

C-3.9 BSS-TS09: Dispute Handling [E.2.1.3.9]

Tables C-3.9-1

Table C-3.9-1. Dispute Handling – Self-Provisioning Orders – Government Initiated Dispute.

Test Scenario	BSS-TS09: Dispute Handling
Test Case ID	BSS-TS09-01
Test Case Description	Government Initiated Dispute [E.2.1.3.9.1]
Requirements Reference(s)	J.2.3; J.2.6.3
Prerequisites	- TO controlled, TO associated, and System Reference data loaded into AT&T's BSS - One or more previously provisioned orders - At least one previously submitted Billing Invoice (BI)
Government Input(s)	- Government issues at least 2 Disputes (D) as defined in RFP Section J.2.6 - Notification to close a dispute after first Dispute Report is issued (see expected outputs)
Expected Output(s)	- Dispute Report (DR) - Reflects open Disputes - A second Dispute Report (DR) - Reflects open and closed Disputes
Acceptance Criteria	- All required CDRLs - Accurate data based on inputs - Correct technical aspects
Data Set Description	Each government-provided test data set will include: - At least two Disputes (D) - Notification to close one or more disputes

C-3.10 BSS-TS10: SLA Management [E.2.1.3.10]

E.2.1.2.2. Tables C-3.10-1 – C-10-2

Table C-3.10-1. SLA Management – SLA Reporting.

Test Scenario	BSS-TS10: SLA Management
Test Case ID	BSS-TS10-01
Test Case Description	SLA Reporting [E.2.1.3.10.1]
Requirements Reference(s)	G.3; J.2.4
Prerequisites	- TO controlled, TO associated, and System Reference data loaded into AT&T's BSS - One or more previously provisioned orders
Government Input(s)	Services to show as SLAs met or missed
Expected Output(s)	SLA Report (SLAR)
Acceptance Criteria	- All required CDRLs - Accurate data based on inputs - Correct technical aspects
Data Set Description	Services by UBI to show as SLAs met or missed

Table C-3.10-2. SLA Management – SLA Credit Request.

Test Scenario	BSS-TS10: SLA Management
Test Case ID	BSS-TS10-02
Test Case Description	SLA Credit Request [E.2.1.3.10.2]
Requirements Reference(s)	G.3; J.2.4; J.2.10.3.1.19
Prerequisites	- TO controlled, TO associated, and System Reference data loaded into AT&T's BSS - One or more previously provisioned orders - At least one previously submitted Billing Invoice (BI) - SLA Report with at least one SLA missed
Government Input(s)	SLA Credit Request (SLACR)
Expected Output(s)	SLA Credit Request Response
Acceptance Criteria	- All required CDRLs - Each CDRL meets requirements
Data Set Description	Each government-provided test data set will include: SLA Credit Request

C-3.11 BSS-TS11: Open-format Reporting [E.2.1.3.11]

Tables C-3.11-1 shows the test case for Open-Format Reporting.

Table C-3.11-1. Open-Format Reporting – Open-Format Reporting: Samples.

Test Scenario	BSS-TS11-01: Open-Format Reporting
Test Case ID	BSS-TS11-01
Test Case Description	Open-Format Reporting: Samples [E.2.1.3.11.1]
Requirements Reference(s)	G.4; G.5; J.2.10.2.1.13; J.2.10.2.1.25; J.2.10.2.1.26
Prerequisites	N/A
Government Input(s)	N/A

Test Scenario	BSS-TS11-01: Open-Format Reporting
Test Case ID	BSS-TS11-01
Test Case Description	Open-Format Reporting: Samples [E.2.1.3.11.1]
Expected Output(s)	- Sample copies of the AT&T's standard reports for: - Monthly Billing Information Memorandum - Trouble Management Incident Performance Report - Describes service outage or degradation that are user initiated and/or automated monitoring created reports - Trouble Management Performance Summary Report
Acceptance Criteria	Each CDRL meets requirements
Data Set Description	N/A

Figure C-3.11-1



Figure C-3.11-1. Sample Open-Format Reporting.

C-3.12 BSS-TS12: Regression Testing [E.2.1.3.12]

C-3.12.1 BSS-TS12-01: Regression Testing [E.2.1.3.12.1]

Table C-3.12-1 shows test cases for Regression Testing.

Table C-3.12-1. Test Case for Regression Testing.

Test Scenario	BSS-TS12: Regression Testing
Test Case ID	BSS-TS12-01
Test Case Description	Regression Testing: Test Cases TBD
Requirements Reference(s)	G.5.5
Prerequisites	AT&T has completed BSS development test and received ATO
Government Input(s)	TBD based on Change Management in RFP G.5.5
Expected Output(s)	TBD based on Change Management in RFP G.5.5
Acceptance Criteria	TBD
Data Set Description	TBD

C-3.13 BSS-TS13: Security Testing [E.2.1.3.13]

C-3.13.1 BSS-TS13-01: Security Testing [E.2.1.3.13.1]

Table C-3.13-1

Table C-3.13-1. Test Case for Security Testing.

Test Scenario	BSS-TS13: Security Testing
Test Case ID	BSS-TS13-01

Test Case Description	Security Testing
Requirements Reference(s)	▪ G.5.6
Prerequisites	▪ Depending on test as defined in RFP Section G.5.6
Government Input(s)	▪ Depending on test as defined in RFP Section G.5.6
Expected Output(s)	▪ Depending on test as defined in RFP Section G.5.6
Acceptance Criteria	▪ AT&T BSS receives ATO
Data Set Description	▪ Depending on test as defined in RFP Section G.5.6

C-4 Test Results [E.2.1.4]

Table C-4-1.

Table C-4-1. Testing Details.

Testing Details
▪ Functional requirements for the Ordering, Billing, Inventory Management, Disputes, SLA Management and Trouble Ticketing Processes as described in RFP Sections G and J.2.
▪ System-to-system data exchange mechanism requirements defined in RFP Section G.5 for each CDRLs defined in RFP Section J.2.
▪ Correct CDRLs are used in the data exchange.
▪ Mandatory data elements for each CDRL defined in RFP Section J.2.10 Data Dictionary are populated and accurate.
▪ Available optional data elements for each CDRL defined in RFP Section J.2.10 Data Dictionary are populated and accurate.
▪ Timely and successful system to system data exchange to meet defined performance SLAs and provisioning intervals.

Figure C-4-1.

C-4.1 Functional Requirements Processes [E.2.1.4]

C-4.1.1 Ordering [E.2.1.4]

See Figure C-4-1

C-4.1.2 Billing [E.2.1.4]

See Figure C-4-1

C-4.1.3 Inventory Management [E.2.1.4]

See Figure C-4-1

C-4.1.4 Disputes [E.2.1.4]

See Figure C-4-1

C-4.1.5 SLA Management [E.2.1.4]

See Figure C-4-1

C-4.1.6 Trouble Ticketing [E.2.1.4]

See Figure C-4-1

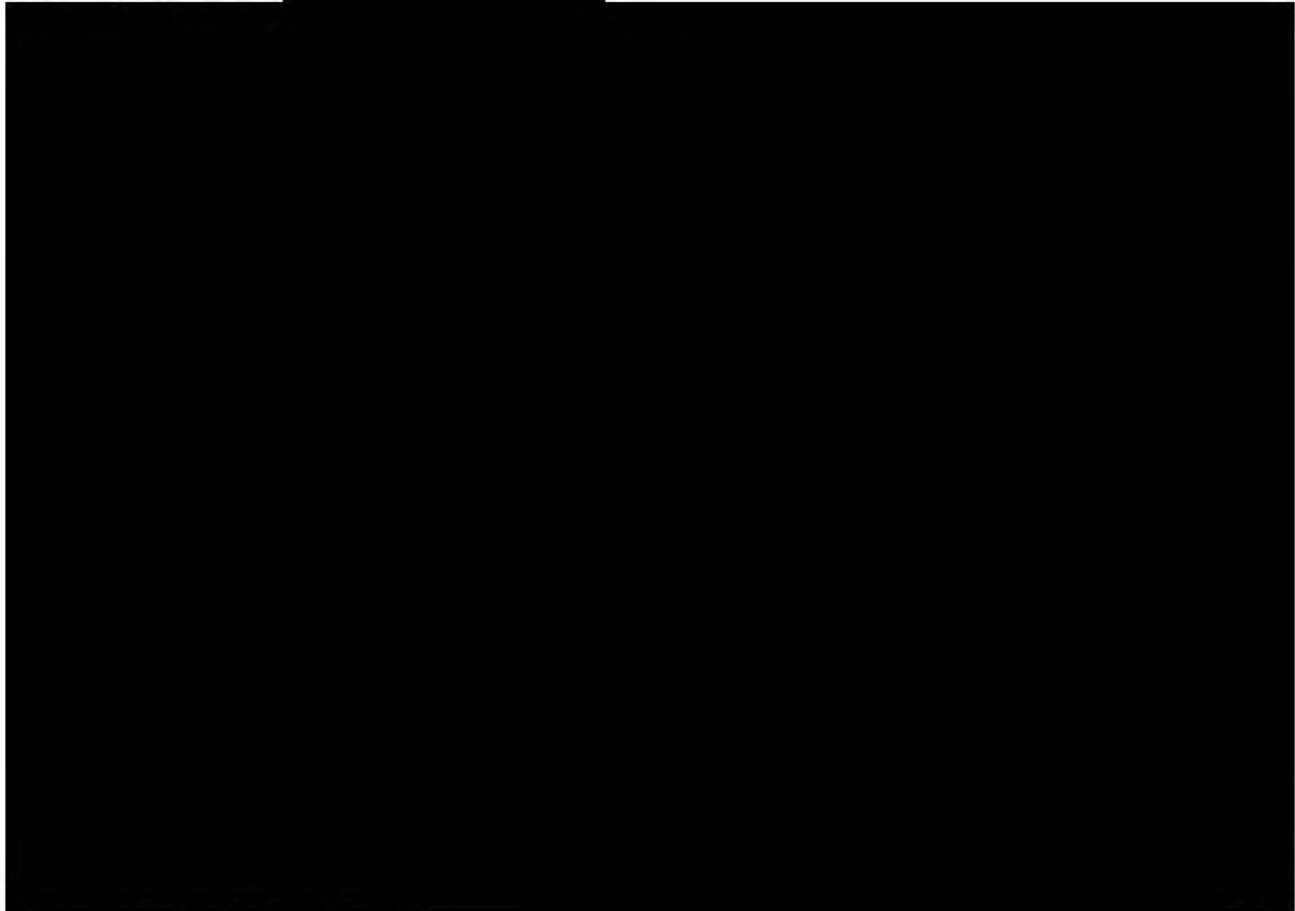
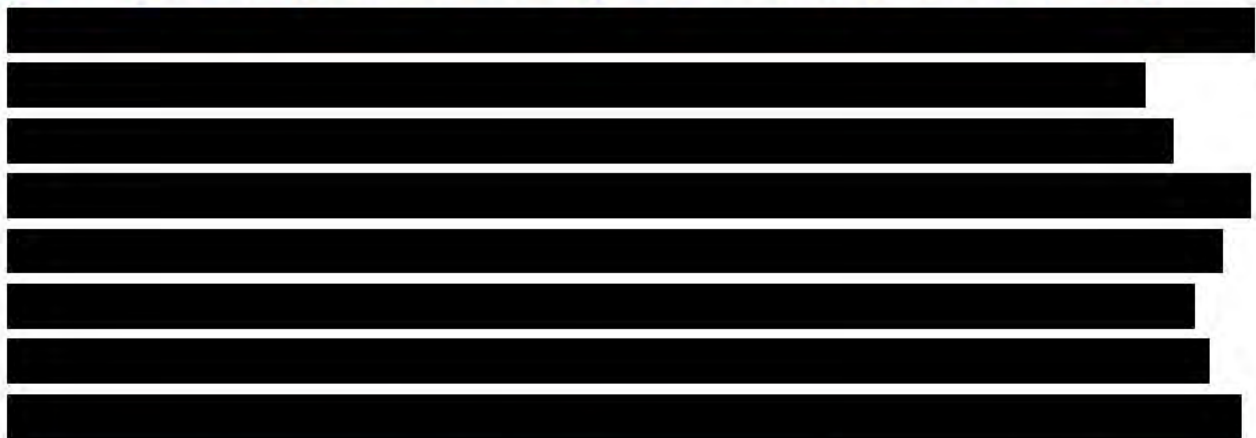


Figure C-4-1. Test Results Report.

C-4.2 System to System Data Exchange Mechanism Requirements [E.2.1.4]



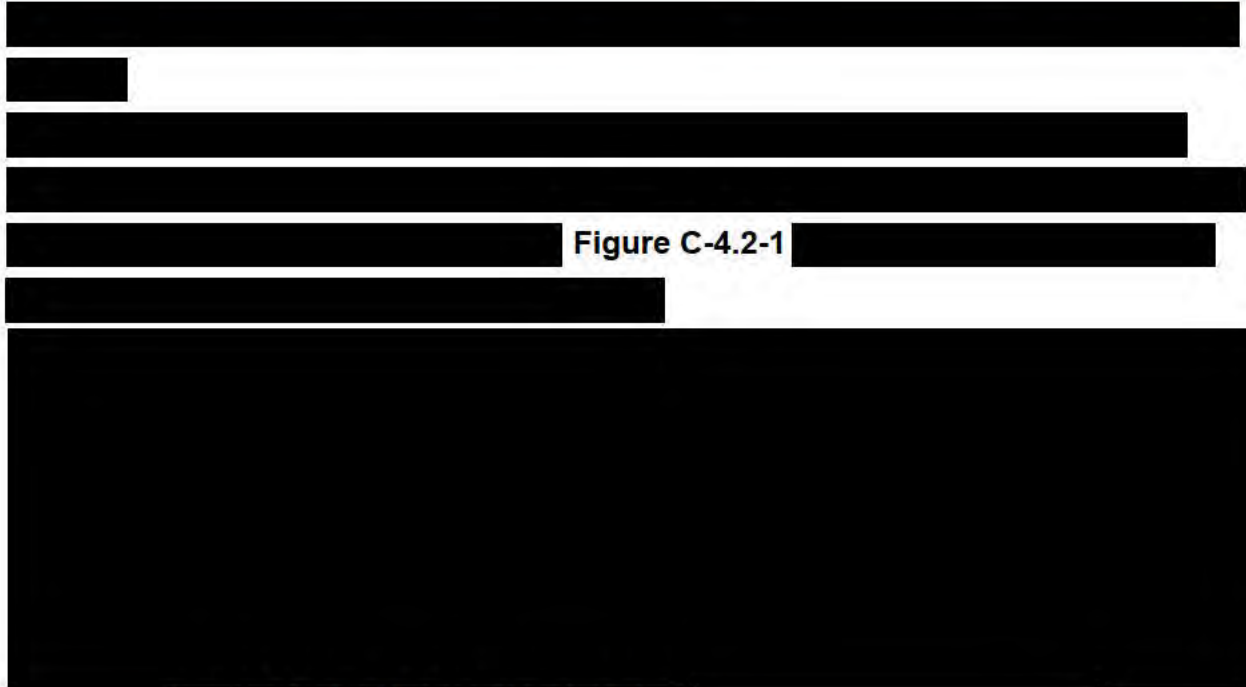


Figure C-4.2-1. CDIP High-Level Process Flow.

C-4.3 Correct CDRLs Used in the Data Exchange [E.2.1.4]



C-4.4 Mandatory Data Elements for Each CDRL Defined in RFP Section J.2.10 Data Dictionary [E.2.1.4]

Upon completion of the test cases,

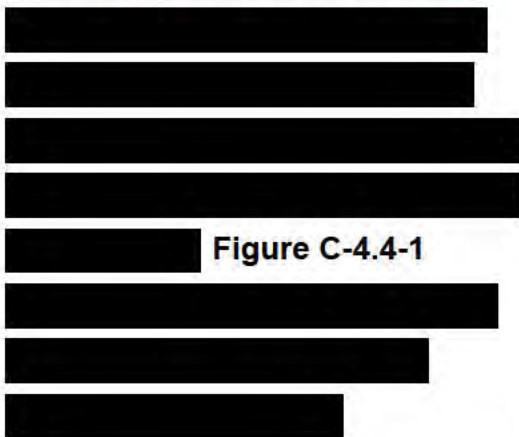


Figure C-4.4-1

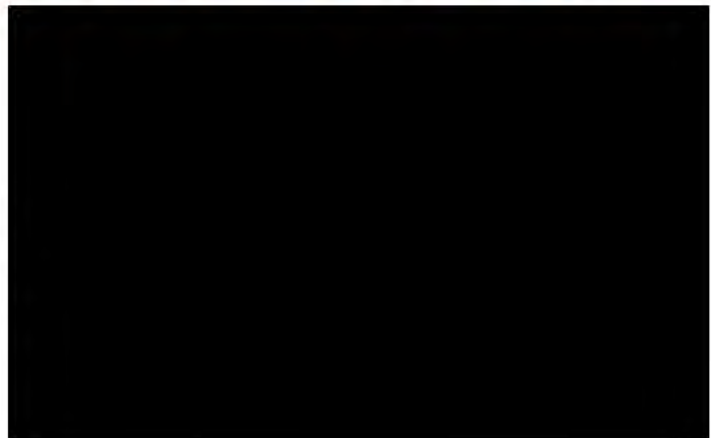


Figure C-4.4-1. Service Order Acknowledgement (SOA) Mandatory Data Elements.

C-4.5 Available Optional Data Elements for Each CDRL Defined in RFP Section J.2.10 Data Dictionary [E.2.1.4]

C-4.6 Timely and Successful System to System Data Exchange to Meet Defined Performance SLAs and Provisioning Intervals [E.2.1.4]

C-4.7 Test Results Minimums [E.2.1.4]

As shown in **Figure C-4-1**,

C-5 Deliverables [E.2.1.5]

The following subsections provide details on our deliverables.

C-5.1 Verification Test Plan for AT&T's BSS [E.2.1.5.1]

Figure C-1-2.

Figure C-5.1-1

Figure C-5.1-1. Draft Timeline.

[REDACTED]

C-5.2 Verification Test Results Report for AT&T's BSS [E.2.1.5.2]

[REDACTED]

[REDACTED]



General Services Administration (GSA)

Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

GS00Q17NSD3000
Appendix D — EIS Verification Test Plan

APPENDIX D — EIS SERVICES VERIFICATION TEST PLAN (EIS TEST PLAN) [L.30; L.30.2.4; M.2.2(3 OF 7); E.2.2]

Introduction — Standard EIS Verification Testing Approach: Verification testing will demonstrate our compliance with the service-specific Key Performance Indicators (KPIs) defined in Section C.2 of the Network Services 2020 Enterprise Infrastructure Solutions (NS2020 EIS) Contract. Each service will have a verification test plan that demonstrates compliance with the KPIs for that service. In this appendix, we describe our approach to performing verification test scenarios as outlined in RFP Section E.2.2.2 and for obtaining government acceptance for each proposed EIS contract services. Test Scenarios are provided by the government in RFP Section E.2.2.2.

Additional Testing: AT&T recognizes that an agency may define additional testing in the TO.

Test and Service Ordering Are Linked: We will perform verification testing on each of our bid NS2020

Figure D-1 illustrates our verification testing and service order process.

Figure D-1. Verification Testing and Service Order Process.

The service-specific test plans summarized in this verification plan — including the scenarios, test cases, and acceptance criteria — will serve as the preliminary NS2020

EIS Contract verification plan. AT&T will conduct the service-specific verification tests. The logistics (i.e., time, locations, resources, etc.) for conducting each service-specific verification tests will be detailed in the service-specific verification test plans tabularized in this appendix.

Fallback Approach: If a test fails in any service verification test, [REDACTED]

New Services: We will develop new EIS test plans, using the process shown in **Figure D-1**, during the life of the NS2020 EIS Contract and, include them in service-specific test plans. Updates to this process and or the service specific verification test plan tables, for any new services will be submitted within any modification proposal.

FedRAMP and NIST Requirements: AT&T will provide GSA-accepted Federal Risk and Authorization Management Program (FedRAMP), National Institute of Standards and Technology (NIST), and supporting authorization certifications for all cloud services we offer. We will conduct cloud services testing according to this plan and Task Order (TO) requirements.

Acceptance and Reporting: When service-specific verification testing is completed and the test results demonstrate compliance with the associated KPIs and acceptance criteria, we will provide the government with the appropriate verification test report. [REDACTED]

AT&T Provides All Necessary Test Equipment: The resources to implement the verification test plan include test location(s), NS2020 service offering, service related equipment (SRE), test equipment, network data collection devices, computers/ workstations, and personnel. We will provide all necessary resources to implement each service-specific verification test plan. We will use data from the verification testing to

Re-Testing: [REDACTED]

[illegible]

Testing Not Applicable: AT&T will identify any service from Section C.2 in which testing is not applicable.

New Services Verification Tests: AT&T will submit updates to this verification plan for any new services that are added due to contract modifications.

The plans also contain Federal Information Security Management Act (FISMA) and FedRAMP compliance requirements. Each service-specific plan is tabulated below.

Access to Government Facilities for Verification Testing: We assume that access to government facilities for verification testing will require, at a minimum, the following information: the government facility location (physical address), procedures for physical access to the government facility (including point of contact for access), a list of AT&T personnel requiring access, the dates when access is required, test cases to be performed at the government facility, and equipment required at the facility to complete the verification testing.

Verification Test Report: After we collect all verification test data, we will record the results for each test case in the verification test case table on a service-specific basis and provide the table to the government. The following tables depict our proposed test plans for the services we are bidding.

D-1 Service Area—Data Service

D-1.1 EIS Test Plan for Virtual Private Network Service (MANDATORY) [L.30.2.4; E.2.2]

Table D-1.1-1. EIS Virtual Private Network Service Test Plan.

EIS Virtual Private Network Service Test Plan	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for All Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and Service Level Agreements (SLAs) of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.

EIS Virtual Private Network Service Test Plan

Table D-1.1-2. VPNS Verification Test Plan Locations and Port Speeds.

Location	Speed	Service Order Number
Location 1		TBD subsequent to award
Location 2		TBD subsequent to award
Location 3		TBD subsequent to award
Location 4		TBD subsequent to award
Location 5		TBD subsequent to award
Location 6		TBD subsequent to award

Figure D-1.1-1. Service Test Plan Process Flow.

VPNS Service Order Information	The following information details the VPNS service order undergoing testing: - Service Order Number: supplied after the agency places the order - Service locations involved with verification testing involves all of the POPs within the AT&T network involved with the transport for the VPNS - Associated Access Arrangement Order Information. The Wireline Access Arrangement order information will be included with the service order information. RFP Section C.2.1.1.4 defines the measurable KPIs between GSA premises routers for a VPNS. However, VPNS do not include a managed premises router component, so verification testing requires only POP-to-POP measurements.
Parameters to be Measured	The awarded services will be delivered based on KPIs and SLAs defined in RFP Section C.2.1.1. The following are the aggregate KPIs as defined in EIS RFP Section C.2.1.1.4, Performance Metrics, with exceptions to the measurements to be verified by the performance of the test cases described in other sections of this service-specific test plan:
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above in this table.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.1.1.4.
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS Test Plans will be developed using the process in Figure D-1 for all new services in the NS2020 EIS Contract.

EIS Virtual Private Network Service Test Plan						
Testing Conditions [E.2.2.1]						
Requirement			Description			
Agency Defines Additional Testing in the TO			As defined in specific TO			
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing			All service testing will be available for government observation, upon request.			
AT&T to Provide all Test Equipment			AT&T will provide all test equipment, hardware, software, and tools for all service testing.			
Test Scenarios [E.2.2.2]						
Requirement			Description			
Service TS-02 [E.2.2.2.1; G.8]			Test as defined in RFP Section E.2.2.2.1			
Test Cases [E.2.2.3; C.2.1.1.4]						
Requirement			Description			
TS-02			Test as defined in RFP Section E.2.2.2.1			
Test Cases Determined by AT&T			The VPNS test plan defines four verification test cases, listed in Table D-1.1-6.			
Table D-1.1-3. Service-Specific Verification Test Cases. [C.2.1.1.4]						
Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable ¹ Result	Actual Result
1	Latency ² CONUS					TBD
2	Latency ² OCONUS					TBD
3	Availability ³ (VPN)—Routine					TBD
4	Availability ³ (VPN)—Critical					TBD
Test Data Sets [E.2.2.4]						
Requirement			Description			
Test Data Sets						

EIS Virtual Private Network Service Test Plan	
Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All verification and acceptance testing results from this plan and as defined in RFP Section E.2.2.5
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval
EIS Testing Report	Provided within 3 days of service installation and testing

D-1.2 EIS Test Plan for Ethernet Transport Service (MANDATORY) [L.30.2.4; E.2.2]

Table D-1.2-1. Ethernet Transport Service Verification Test Plan.

Ethernet Transport Service	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and Service Level Agreements (SLAs) of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	

Table D-1.2-2. Ethernet Transport Service Locations and Speeds.

Location	Speed	Service Order Number
Location 1		TBD subsequent to award
Location 2		TBD subsequent to award
Location 3		TBD subsequent to award
Location 4		TBD subsequent to award

Parameters to be Measured	The following aggregate KPIs, as defined in section C.2.1.2.4 of the EIS RFP, will be verified by the performance of the test cases described in this service specific test plan:
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.1.2.4.

Ethernet Transport Service	
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in Figure D-1 for all new services in the NS2020 EIS Contract.
Testing Conditions [E.2.2.1]	
Requirement	Description
Agency Defines Additional Testing in TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	All service testing will be available for government observation, upon request.
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing.
Test Scenarios (Selected per Service Requirement) [E.2.2.2]	
Requirement	Description
TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1
Test Cases [E.2.2.3; C.2.1.2.4]	
Requirement	Description
TS-02	Test as defined in RFP Section E.2.2.2.1
Test Cases	The Ethernet Transport service test plan defines nine test cases listed in Table D-1.2-3.

Table D-1.2-3. Service Specific Verification Test Cases. [C.2.1.2.4]

Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result	Actual Result
1	Availability (ETS) Routine—Single Connection					TBD
2	Availability (ETS) Critical—Double Connection					TBD
3	Latency (ETS) (CONUS)					TBD
4	Latency (ETS) (OCONUS)					TBD
5	Jitter (packet)—Routine					TBD
6	Grade of Service (GOS) (packet delivery rate)—Routine					TBD
7	Grade of Service (packet delivery rate)—Critical					TBD
8	Grade of Service (packet loss = 1—GOS)—Routine					TBD
9	Grade of Service (packet loss = 1—GOS)—Critical					TBD

Ethernet Transport Service	
Test Data Sets Determined by AT&T [E.2.2.4]	
Requirement	Description
Test Data Sets	
Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All test results, acceptance, and compliance reporting as defined in RFP Section E.2.2.5
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval. Updates for new services added to contract.
EIS Testing Report	

D-1.3 EIS Test Plan for Optical Wavelength Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-1.3-1. Optical Wavelength Service Verification Test Plan.

Optical Wavelength Service	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and Service Level Agreements (SLAs) of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	
Parameters to be Measured	The following aggregate Key Performance Indicators (KPIs), as defined in section C.2.1.3.4 of the EIS RFP, will be verified by the performance of the test cases described in this service specific test plan.

Table D-1.3-2. Optical Wavelength Service Parameters.

Location	Speed	Service Order Number
Location 1		TBD subsequent to award
Location 2		TBD subsequent to award
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above in this table.	
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.1.3.4.	

Optical Wavelength Service						
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure						
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in Figure D-1 for all new services in the NS2020 EIS Contract					
Testing Conditions [E.2.2.1]						
Requirement	Description					
Agency Defines Additional Testing in the TO	As defined in the specific TO					
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.					
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing.					
Test Scenarios [E.2.2.2]						
Requirement	Description					
Service TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1					
Test Cases Determined by AT&T [E.2.2.3; C.2.1.3.4]						
Requirement	Description					
TS-02	Test as defined in RFP Section E.2.2.2.1					
Test Cases	The Optical Wavelength Service test plan defines two test cases listed in Table D-1.3-2. The following information provides the details on the OWS service order that is undergoing verification testing: ▪ Service Order Number: supplied after the agency places the order ▪ Service Locations Involved with Verification Testing: involves all of the POPs within the AT&T network involved with the transport for the OWS ▪ Associated Access Arrangement Order Information. The Wire line Access Arrangement order information will be included with the service order information					
Table D-1.3-3. Test Cases [C.2.1.3.4]						
Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result	Actual Result
1	Availability(OWS over WDM) — Routine					TBD
2	Availability (OWS over WDM) — Critical					TBD
Test Data [E.2.2.4]						
Requirement			Description			
Test Data Sets Determined by AT&T						

Optical Wavelength Service	
Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All test results, acceptance, and compliance reporting as defined in RFP Section E.2.2.5
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval
EIS Testing Report	Provided within 3 days of service installation and testing

D-1.4 EIS Test Plan for Private Line Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-1.4-1. Private Line Service Verification Test Plan.

Private Line	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and Service Level Agreements (SLA) of each type of this service using processes in this table and assumptions in Appendix introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	

Private Line

Figure D-1.4-1. Service Test Plan Process Flow.

Parameters to be Measured	Demonstrate that awarded service is delivered based on KPIs and SLAs defined in RFP Section C.2.1.4. The following aggregate KPIs, as defined in Section C.2.1.4.4 Performance Metrics of the EIS RFP, will be verified by the performance of the test cases described in this service-specific test plan. - Availability (SDP-to-SDP) — Routine — 99.9% - Availability (SDP-to-SDP) — Critical — 99.99% - Availability (POP-to-POP) — Routine — 99.9% - Availability (POP-to-POP) — Critical — 99.99%
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.1.4.4
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in Figure D-1 for all new services during the life of the NS2020 EIS Contract and added to service-specific test plans.

Testing Conditions [E.2.2.1]

Requirement	Description
Agency Defines Additional Testing in the TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.
AT&T to Provide all Test Equipment	AT&T will provide all required test sets/equipment/resources required for the PLS verification testing.

Test Scenarios (scenarios selected per service requirement) [E.2.2.2]

Requirement	Description
Service TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1

Test Cases [E.2.2.3; C.2.1.4.4]

Requirement	Description
Test Cases	The test cases in Table D-1.4-2 cover POP-to-POP and SDP-to-SDP availability. The metrics are the same and the SDP-to-SDP test will include the POP-to-POP-test in each case.

Table D-1.4-2. Private Line Service Test Cases. [C.2.1.4.4]

Test Case	KPI	AQL	Test Case Description ²	Test Period ³	Acceptable Result ¹	Actual Result
1	Availability SDP-to-SDP Routine					TBD
2	Availability SDP-to-SDP Critical					TBD



Private Line	
Private Line Verification Testing Schedule	This subsection outlines the schedule for verification testing. Of particular interest are schedule dates associated with the following: ▪ Forecasted verification test plan start date ▪ Forecasted verification test plan end date ▪ Schedule dates when access to government buildings is required (must fall within the start and end date of the forecasted test dates)
Test Data Sets Determined by AT&T [E.2.2.4]	
Requirement	Description
Test Data Sets Determined by AT&T	
Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All test results, acceptance, and compliance reporting as defined in RFP Section E.2.2.5
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval
EIS Testing Report	Provided within 3 days of service installation and testing.



D-1.5 EIS Test Plan for Synchronous Optical Network Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-1.5-1. Synchronous Optical Network Service Verification Test Plan.

Synchronous Optical Network	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	

Table D-1.5-2. SONET Port Speeds.

Location	Speed	Service Order Number
Location 1		TBD subsequent to award
Location 2		TBD subsequent to award
Location 3		TBD subsequent to award
Location 4		TBD subsequent to award

Parameters to be Measured	The following aggregate KPIs, as defined in RFP Section C.2.1.5.4 of the EIS RFP, will be verified by the performance of the test cases described in this service specific test plan: - Availability (SONETS) (SDP-to-SDP) — Routine - Availability (SONETS) (SDP-to-SDP) — Critical
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.1.5.
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in Figure D-1 for all new services during the life of the NS2020 EIS Contract and added to service-specific test plans.
Testing Conditions [E.2.2.1]	
Requirement	Description
Agency Defines Additional Testing in the TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.
AT&T to Provide all Test Equipment	AT&T will provide all test and related infrastructure equipment, hardware, and software for all service testing.

Test Scenarios (scenarios selected per service requirement) [E.2.2.2]						
Requirement		Description				
Service TS-02 [E.2.2.2.1; G.8]		Test as defined in RFP Section E.2.2.2.1				
Test Cases [E.2.2.3; C.2.1.5.4]						
Requirement		Description				
TS-02		Test as defined in RFP Section E.2.2.2.1 ▪ Test Case #1 (determined by AT&T) [E.2.2.3; E.2.2.2:] — The SONET test plan defines two test cases listed in Table D-1.5-3.				

Table D-1.5-3. Synchronous Optical Network Test Cases. [C.2.1.5.4]						
Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result	Actual Result
1	Availability (SONET) (SDP-to-SDP) — Routine	≥ 99.8%			≥ 99.8%	TBD
2	Availability (SONET) (SDP-to-SDP) — Critical	≥ 99.999%			≥ 99.999%	TBD

The following information provides the details on the SONET service order that is undergoing verification testing:

- **Service Order Number:** This will be supplied after the agency places the order.
- **Service Locations Involved with Verification Testing:** This involves all of the POPs within the AT&T network involved with the transport for the SONET.
- **Associated Access Arrangement Order Information:** The Wireline Access Arrangement order information will be included with the service order information. RFP Section C.2.1.5.4 defines the measurable KPIs between agency premise routers for SONET.

SONET Service Testing Schedule — The SONET availability performance data is continuously collected and recorded through the network elements in the AT&T SONET network. As such, a testing schedule is not required. Averages from the previous month will be available within the first few days of the new month.

SONET Service Verification Testing Resources — The network's availability data is gathered by internal network monitoring and recorded to an Internet portal. No further resources are required to provide verification test data.

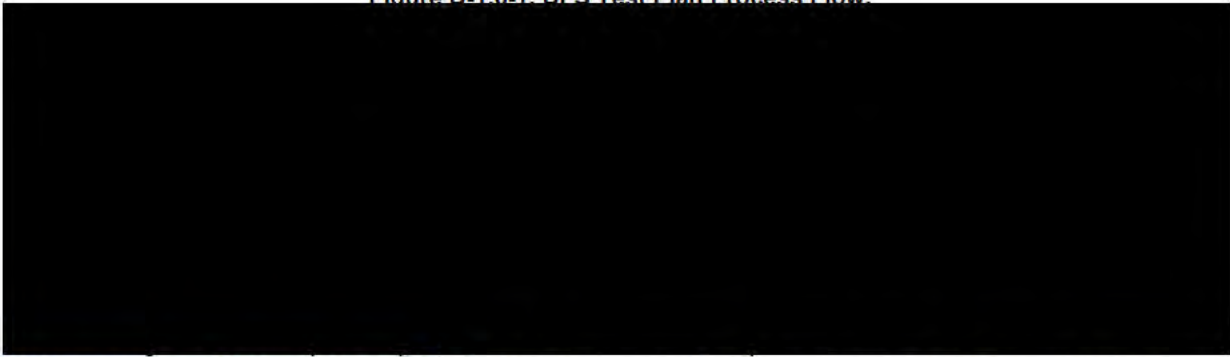
Test Data Sets Determined by AT&T [E.2.2.4]	
Requirement	Description
Test Data Sets	

Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All test results, acceptance, and compliance reporting as defined in RFP Section E.2.2.5

Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval
EIS Testing Report	Provided within 3 days of service installation and testing.

D-1.6 EIS Test Plan for Dark Fiber Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-1.6-1. Dark Fiber Service Verification Test Plan.

Dark Fiber	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	
Figure D-1.6-1. DES Test Plan Process Flow. 	
Parameters to be Measured [E.2.2.1]	The following aggregate KPIs, as defined in RFP Section C.2.1.6.4 Performance Metrics of the EIS RFP, will be verified by the performance of the test cases described in this service specific test plan. ▪ Attenuation Coefficient Single Mode Optical Fiber (SMF) (1550 nm) ▪ Attenuation Coefficient SMF (1310 nm) ▪ Attenuation Coefficient Multi-Mode Optical Fiber (MMF) 850 nm (50/125 μm) ▪ Attenuation Coefficient MMF 1300 nm (50/125 μm) ▪ Polarization Mode Dispersion at 1550 nm (Inter-City Networks) ▪ Polarization Mode Dispersion (Intra-City Networks) ▪ Chromatic Dispersion at 1550nm ▪ Reflectance Events (all events) ▪ Connectors Loss SMF ▪ Fusion Splicing Loss SMF
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.1.6.4
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	

Dark Fiber						
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in Figure D-1 for new services during the NS2020 EIS Contract and added to service-specific test plans.					
Testing Conditions [E.2.2.1]						
Requirement	Description					
Agency Defines Additional Testing in the TO	As defined in the specific TO					
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.					
AT&T to Provide all Test Equipment	AT&T will provide all test and related infrastructure equipment, hardware, and software for all service testing.					
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]						
Requirement	Description					
Service TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1					
Service TS-03 [E.2.2.2.1]	Test as defined in RFP Section E.2.2.2.1 Verification Testing of Dark Fiber Services					
Test Cases [E.2.2.3; C.2.1.6.4]						
Requirement	Description					
Service TS-02 Service TS-03	The DFS test plan defines 11 verification test cases, as listed in Table D-1.6-2 . Dark fiber will be tested in three wavelength bands: 850nm, 1310nm, and 1550nm as required by the KPIs and the specific TO (850nm and 1310nm for multimode fiber) and (1310nm and 1550nm for single mode fiber).					
Table D-1.6-2. Dark Fiber Service Verification Test Cases. [C.2.6.1.4]						
Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result	Actual Result
1	Attenuation Coefficient SMF (1550 nm)					TBD
2	Attenuation Coefficient SMF (1310 nm)					TBD
3	Attenuation Coefficient MMF 850 nm (50/125 μm)					TBD
4	Attenuation Coefficient MMF 1300 nm (50/125 μm)					TBD
5	Polarization Mode Dispersion (PMD) at 1550 nm (Inter-City Networks)					TBD

						TBD
						TBD
						TBD
						TBD
						TBD
						TBD
Test Data Sets Determined by AT&T [E.2.2.4]						
Requirement		Description				
Test Data Sets						
Test Results and Acceptance [E.2.2.5]						
Requirement		Description				
Test Results and Acceptance [E.2.2.5; C.2]		All test results, acceptance, and FedRAMP and FISMA compliance reporting as defined RFP Section E.2.2.5				
Deliverables [E.2.2.6]						
Requirement		Description				
EIS Test Plan		Provided for government approval				
EIS Testing Report		Provided within 3 days of service installation and testing				

D-1.7 EIS Test Plan for Internet Protocol Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-1.7-1. Internet Protocol Service Verification Test Plan.

Internet Protocol Service	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	

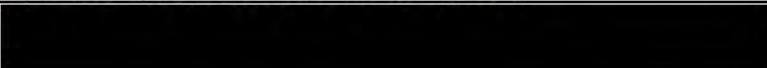
Table D-1.7-2.

Internet Protocol Service

Table D-1.7-2. IPS Port Speeds.

Location	Speed	Service Order Number
TBD	DS1	TBD
TBD	100 Mbps	TBD

These two test cases cover Time Division Multiplexing (TDM) and SONET access to IPS and Ethernet access to IPS.

Parameters to be Measured	The following aggregate Key Performance Indicators (KPI), as defined in RFP Section C.2.1.7.4 of the EIS RFP, will be verified by the performance of the test cases described in this service specific test plan: 
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.1.7.4
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in Figure D-1 for all new services during the NS2020 EIS Contract and added to service-specific test plans.

Testing Conditions [E.2.2.1]

Requirement	Description
Agency Defines Additional Testing in TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by Government representatives, upon notice to AT&T.
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing.

Test Scenarios (scenarios selected per service requirement) [E.2.2.2]

Requirement	Description
Service TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1

Test Cases [E.2.2.3; C.2.1.7.4]

Requirement	Description
TS-02	Test as defined in RFP Section E.2.2.2.1
	Test Case #1 [E.2.2.3; E.2.2.2; determined by AT&T]. The IPS test plan defines six (6) verification test cases, listed in Table D-1.7-2.
	Internet Protocol Service Testing Schedule. The IPS Latency and GOS performance data is continuously collected and recorded through the probes in the AT&T IPS network. As such, a testing schedule is not required. Previous month averages will be available within the first few days of the new month. The IPS Port Availability performance data is collected via an AT&T trouble reporting system which aggregates customer ticket data on a monthly basis and averages port availability from the data. As the data

Internet Protocol Service	
	is provided from the trouble reporting system, a testing schedule is not required. Previous month averages will be available within the first few days of the new month.
	Internet Protocol Service Verification Testing Resources. The network's Latency and GOS data is gathered by network probes and recorded to an Internet portal. The portal is http://ipnetwork.bgtmo.ip.att.net/pws/averages.html . No further resources are required to provide Verification Test data. The port availability data will be provided by the AT&T trouble reporting system through internal AT&T methods and procedures.

Table D-1.7-3. IPS Verification Test Cases. The test cases that make up the IPS Verification Test Plan are presented in a table format. A blank space is provided to record the actual results. [C.2.1.7.4]

Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result	Actual Result
1	Availability (Port) — Routine ²					
2	Availability (Port) — Critical ²					
3	Latency (CONUS) — Routine ³					
4	Latency (CONUS) — Critical ³					
5	GOS (Data Delivery Rate) — Routine ⁴					
6	GOS (Data Delivery Rate) — Critical ⁴					

Test Data Sets Determined by AT&T [E.2.2.4]	
Requirement	Description
Test Data Sets Determined by AT&T	Monthly availability, latency, jitter, and GOS data provided in Excel, PowerPoint, and/or PDF formats
Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval
EIS Testing Report	Provided within 3 days of service installation and testing

D-1.8 EIS Test Plan for Broadband Internet Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-1.8-1. Broadband Internet Service Verification Test Plan.

Broadband Internet Service	
General Testing Requirements [E.2.2.1]	
Requirement	Description

Broadband Internet Service	
Verification and Acceptance Testing Approach for all Awarded EIS Services	
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	Monthly historical time to restore metrics will be calculated using internal applications. Content refresh times will be measured on a pseudo-random basis. Availability metric is noted but will not be measured as the service lists the Availability KPI as best effort.
Parameters to be Measured	
Measurement Procedure	Calculate time to restore via trouble ticket data for a specified time period.
Acceptance (Pass/Fail) Criteria	
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	If a test fails in any service verification test, appropriate service-specific remediation will take place, followed by re-testing.
Development of EIS Test Plan for all New Services during the Life of the Contract	
Testing Conditions [E.2.2.1]	
Requirement	Description
Testing Conditions	Business as usual for monthly operations and trouble ticket collection intervals
Agency Defines Additional Testing in TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing.
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]	
Requirement	Description
Service TS-01 [E.2.2.2.1]	
Service TS-02 [E.2.2.2.1; G.8]	
Test Cases [E.2.2.3; C.2.5.4.4]	
Requirement	Description
Test Cases	
TS-01	
Test Data Sets Determined by AT&T [E.2.2.4]	
Requirement	Description
Test Data Sets Determined by AT&T	Trouble ticket records and results (in units of minutes and seconds) of pseudo-random content refresh time tests

Broadband Internet Service	
Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All test results, acceptance, and compliance reporting as defined in RFP Section E.2.2.5
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	
EIS Testing Report	

D-2 Service Area: Voice Service

D-2.1 Internet Protocol Voice Service (VOICE MANDATORY) [L.30.2.4; E.2.2]

Table D-2.1-1. Internet Protocol Voice Service Verification Test Plan.

Internet Protocol Voice	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	

Table D-2.1-1.

Table D-2.1-2. IPVS Access Speeds.

Location	Speed	Service Order Number
Location 1		TBD subsequent to award

The IPVS verification testing involves testing the IPVS network from network Point Of Presence (POP) to another POP (POP-to-POP), where the POPs are the closest entry point from agency locations to the network, and use of voice quality monitoring equipment to verify Grade of Service (GOS).

IPVS Service Order Information — The following information provides the details on the IPVS service order that is undergoing verification testing.

- **Service Order Number:** This will be supplied after the agency places the order
- **Service Locations Involved with Verification Testing:** This involves the all of the POPs within the AT&T network involved with the transport for the IPVS.
- **Associated Access Arrangement Order Information:** The Wireline Access Arrangement order information will be included with the service order information

RFP Section C.2.2.1.4 defines the measurable KPIs between agency premise routers for an IPVS.

Parameters to be Measured	The following aggregate KPIs, as defined in RFP Section C.2.2.1.4 Performance Metrics of the EIS RFP, with exception to the measurements to be verified by the performance of the test cases described other sections of this service specific test plan.
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.2.1
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in Figure D-1 for all new services during the NS2020 EIS Contract and added to service-specific test plans.

Internet Protocol Voice						
Testing Conditions [E.2.2.1]						
Requirement		Description				
Agency Defines Additional Testing in TO		As defined in the specific TO				
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing		EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.				
AT&T to Provide all Test Equipment		AT&T provides all test equipment, hardware, software and analysis tools for all service testing.				
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]						
Requirement		Description				
Service TS-02 [E.2.2.2.1; G.8]		Test as defined in RFP Section E.2.2.2.1				
Test Cases [E.2.2.3; C.2.2.1.4]						
Requirement		Description				
TS-02		Test as defined in RFP Section E.2.2.2.1				
		Test Cases [E.2.2.3; E.2.2.2; determined by AT&T]. The IPVS test plan defines six verification test cases, listed in the table format below.				
Table D-2.1-3. IPVS Verification Test Cases. The test cases that make up the IPVS verification test plan are presented in a table format.[C.2.2.1.4]						
Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result ¹	Actual Result
1	Latency — Routine ²					TBD
2	Grade of Service (Packet Loss) — Routine					TBD
3	Availability — Routine					TBD
4	Availability — Critical					TBD
5	Jitter — Routine					TBD
6	Voice Quality — Routine ³					TBD
¹ An "Acceptable Result" occurs when each test case results in an actual result that meets or exceeds the defined AQL.						
² IPVS Testing Schedule — The IPVS Latency and Availability performance data is continuously collected and recorded through the probes in the AT&T IPVS network. As such, a testing schedule is not required. Previous month averages will be available within the first few days of the new month.						
³ IPVS Verification Testing Resources — Voice quality monitors will gather Mean Opinion Score (MOS) data. The network's Latency and Availability data is gathered by network probes and recorded to an Internet portal. No further resources are required to provide Verification Test data.						
Test Data Sets Determined by AT&T [E.2.2.4]						
Requirement		Description				
Test Data Sets Determined by AT&T						

Internet Protocol Voice	
Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All test results, acceptance and compliance reporting as defined in RFP Section E.2.2.5
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval
EIS Testing Report	Provided within 3 days of service installation and testing

D-2.2 EIS Test Plan for Circuit Switched Voice Service [L.30.2.4; E.2.2]

Table D-2.2-1.

[illegible]

Requirement		Description				
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]						
Requirement		Description				
Service TS-02 [E.2.2.2.1; G.8]						
Test Cases [E.2.2.3; C.2.2.2.4]						
Requirement		Description				
TS-02						
		Table D-2.2-2.				
Table D-2.2-2.						
Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result	Actual Result
1	Availability — POP-to-POP — Routine					TBD
2	Availability — SDP-to-SDP: Routine					TBD
3	Availability — SDP-to-SDP: Critical					TBD
4	Grade of Service (Call Blockage SDP-to-SDP) Routine					TBD
5	Grade of Service (Call Blockage POP-to-POP) Routine					TBD
6	Grade of Service (Call Blockage) Critical					TBD
Test Data Sets Determined by AT&T [E.2.2.4]						
Requirement		Description				
Test Data Sets Determined by AT&T						
Test Results and Acceptance [E.2.2.5]						
Requirement		Description				
Test Results and Acceptance						

Deliverables [E.2.2.6]			
Requirement		Description	

D-2.3 EIS Test Plan for Toll Free Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-2.3-1. Toll Free Service Verification Test Plan.

Toll Free Service	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	
Parameters to be Measured	The following aggregate Key Performance Indicator (KPI), as defined in RFP Section C.2.2.3.4 of the EIS RFP, will be verified by the performance of the test cases described in this service specific test plan.
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.2.3
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans are developed using the process in Figure D-1 for all new services during the life of the NS2020 EIS Contract and incorporated into service specific test plans.
Testing Conditions [E.2.2.1]	
Requirement	Description
Agency Defines Additional Testing in TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.

Toll Free Service						
AT&T to Provide all Test Equipment		AT&T provides all test equipment, hardware, and software, for all service testing.				
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]						
Requirement		Description				
Service TS-02 [E.2.2.2.1; G.8]		Test as defined in RFP Section E.2.2.2.1				
Test Cases [E.2.2.3; C.2.2.3.4]						
Requirement		Description				
TS-02						
		Test Cases [E.2.2.3; E.2.2.2] The TFS test plan defines five (5) verification test cases in Table D-2.3-2.				
Table D-2.3-2. Toll Free Service Verification Test Cases. The test cases that make up the Toll-Free Service verification test plan are presented in a table format.[C.2.2.3.4]						
Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result	Actual Result
1	Availability — POP-to-POP — Routine					TBD
2	Availability — POP-to-terminating SDP: Routine					TBD
3	Availability — POP-to-terminating SDP: Critical					TBD
4	Grade of Service (Call Blockage) Routine					TBD
5	Grade of Service (Call Blockage) Critical					TBD
The schedule for verification testing is explained in the Table D-2.3-2. However, by using historical data, AT&T can accelerate the testing schedule. Toll Free Service Verification Testing Resources — Existing databases and software tools will be used to retrieve and aggregate the raw data for analysis.						
Test Data Sets Determined by AT&T [E.2.2.4]						
Requirement		Description				
Test Data Sets Determined by AT&T						
Test Results and Acceptance [E.2.2.5]						
Requirement		Description				
Test Results and Acceptance		All test results, acceptance, and standards compliance reporting as defined in RFP Section E.2.2.5				
Deliverables [E.2.2.6]						
Requirement		Description				
EIS Test Plan		Provided for government approval				
EIS Testing Report		Provided within 3 days of service installation and testing				

D-2.4 EIS Test Plan for Circuit Switched Data Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-2.4-1.

General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	
Development of EIS Test Plan	
Test Methodology	
Parameters to be Measured	
Measurement Procedure	
Acceptance (Pass/Fail) Criteria	
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	
Testing Conditions [E.2.2.1]	
Requirement	Description
Agency Defines Additional Testing in TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, and software, for all service testing.
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]	
Requirement	Description

Service TS-02 [E.2.2.2.1; G.8]		Test as defined in RFP Section E.2.2.2.1				
Test Cases [E.2.2.3; C.2.2.3.4]						
Requirement		Description				
TS-02		Table D-2.4-2.				
Table D-2.4-2.						
Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result	Actual Result
1	Availability — POP-to-POP — Routine					TBD
2	Availability — SDP-to-SDP: Routine					TBD
3	Availability — SDP-to-SDP: Critical					TBD
4	Grade of Service (Call Blockage SDP-to-SDP) Routine					TBD
5	Grade of Service (Call Blockage POP-to-POP) Routine					TBD
6	Grade of Service (Call Blockage SDP-to-SDP & POP-to-POP) Critical					TBD
Test Data Sets Determined by AT&T [E.2.2.4]						
Requirement		Description				
Test Data Sets Determined by AT&T						
Test Results and Acceptance [E.2.2.5]						
Requirement		Description				
Test Results and Acceptance						
Deliverables [E.2.2.6]						
Requirement		Description				
EIS Test Plan						
EIS Testing Report						

D-3 Service Area: Contact Center Service

D-3.1 EIS Test Plan for Contact Center Service (OPTIONAL) [L.30.2.4; E.2.2]

Contact Center	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	[REDACTED]
Parameters to be Measured	Demonstrate that awarded services are delivered based on KPIs and SLAs defined in RFP Section C.2.3.1
Measurement Procedure	Review trouble ticket open and closure intervals on a monthly basis. Calculate total downtime and derived availability.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.3.1.5
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	[REDACTED]
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in Figure D-1 for all new services during the life of the EIS contract and added to service-specific test plans.
Testing Conditions [E.2.2.1]	
Requirement	Description
Testing Conditions	Business as usual for monthly operations and trouble ticket collection intervals
Agency Defines Additional Testing in TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.
AT&T to Provide all Test Equipment	AT&T provides all test and related infrastructure equipment, hardware, software for all service testing.
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]	
Requirement	Description
Service TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1
Test Cases [E.2.2.3; C.2.3.1.7]	
Requirement	Description
Test Cases [E.2.2.3; C.2.3.1.7] TS-02	[REDACTED]
[REDACTED]	[REDACTED]
Requirement	[REDACTED]

Contact Center	
Test Data Sets (AT&T Determined)	
Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All test results, acceptance, and compliance reporting as defined in RFP Section E.2.2.5
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval
EIS Testing Report	Provided within 3 days of service installation and testing

D-4 Service Area: Colocated Hosting Service

D-4.1 EIS Test Plan for Data Center Service/Colocated Hosting Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-4.1-1. Colocated Hosting Service Verification Test Plan.

Colocated Hosting	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	
Parameters to be Measured	Demonstrate that awarded services are delivered based on KPIs and SLAs defined in RFP Section C.2.4
Measurement Procedure	Review trouble ticket open and closure intervals on a monthly basis. Calculate total downtime and derived availability.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.4.5.1
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in Figure D-1 for all new services during the life of the NS2020 EIS Contract and added to service-specific test plans.
Testing Conditions [E.2.2.1]	
Requirement	Description
Testing Conditions	Business as usual for monthly operations and trouble ticket collection intervals
Agency Defines Additional Testing in the TO	As defined in the specific Task Order
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing.
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]	

Colocated Hosting	
Requirement	Description
Service TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1
Test Cases [E.2.2.3; C.2.4.5.1]	
Requirement	Description
Test Cases	
TS-02	Test as defined in RFP Section E.2.2.2.1
Test Data Sets Determined by AT&T [E.2.2.4]	
Requirement	Description
Test Data Sets Determined by AT&T	Trouble ticket records
Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All test results, acceptance, and compliance reporting as defined in RFP Section E.2.2.5
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval
EIS Testing Report	Provided within 3 days of service installation and testing

D-5 Service Area: Cloud Service

D-5.1

[illegible]

[illegible]

Table D-5.2-1 EIS Test Plan for Platform as a Service

Platform as a Service	
General Testing Requirements [E.2.2.1]	
Requirement	Description

[illegible]

[illegible]

Table D-5.3-1 Software as a Service Verification Test Plan

[illegible]

[illegible]

Table D-5.4-1. Content Delivery Verification Test Plan.

Content Delivery	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	
Parameters to be Measured	Demonstrate that awarded services are delivered based on KPIs and SLAs defined in RFP Section C.2.5.4
Measurement Procedure	Calculate availability for on a monthly basis and compare against the [REDACTED] based on events tracked by trouble tickets.

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

D-6 Service Area: Wireless Service

D-6.1 EIS Test Plan for Wireless Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-6.1-1. Wireless Service Verification Test Plan.

Wireless Service	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	
Parameters to be Measured	The following aggregate KPI, as defined in RFP Section C.2.6.4.1 of the EIS RFP, will be verified by the performance of the test cases described in this service specific test plan: Availability is calculated as the average service availability of access to the AT&T's network from the AT&T's cell site.
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.6.4.1
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in Figure D-1 for all new services during the life of the NS2020 contract and added to service-specific test plans.
Testing Conditions [E.2.2.1]	
Requirement	Description
Agency Defines Additional Testing in TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing.

Wireless Service		
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]		
Requirement	Description	
Service TS-02 [E.2.2.2.1;G<8]	Test as defined in RFP Section E.2.2.2.1	
Test Cases [E.2.2.3; C.2.6.4.1]		
Requirement	Description	
TS-02		
Test Data Sets Determined by AT&T [E.2.2.4]		
Requirement	Description	
Test Data Sets Determined by AT&T		
Test Results and Acceptance [E.2.2.5]		
Requirement	Description	
Test Results and Acceptance	All test results, acceptance and standards compliance reporting as defined in RFP Section E.2.2.5	
Deliverables [E.2.2.6]		
Requirement	Description	
EIS Test Plan	Provided for government approval	
EIS Testing Report	Provided within	installation and testing

D-7 Service Area: Commercial Satellite Communication Service (OPTIONAL)
[C.1.8.1]

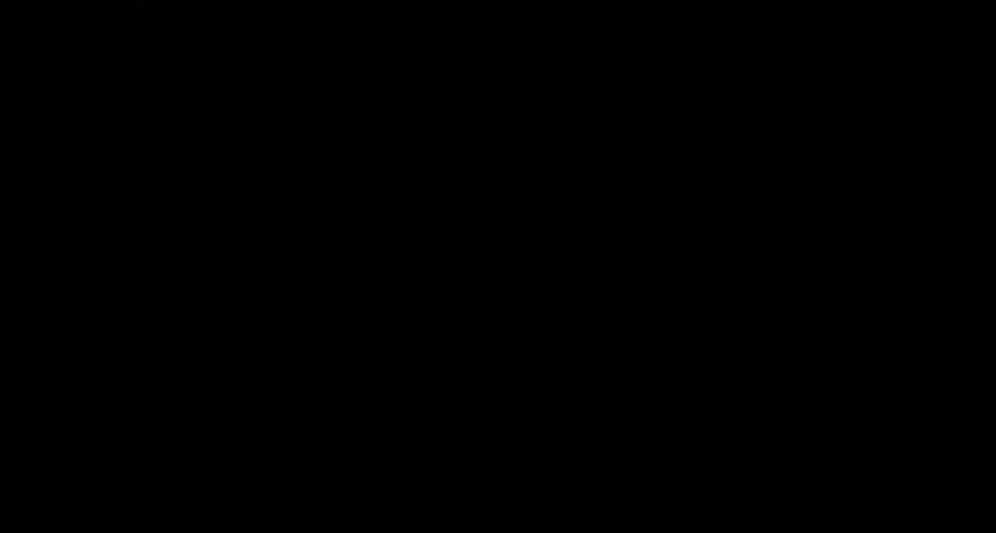
D-7.1

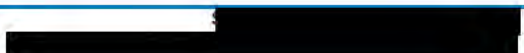
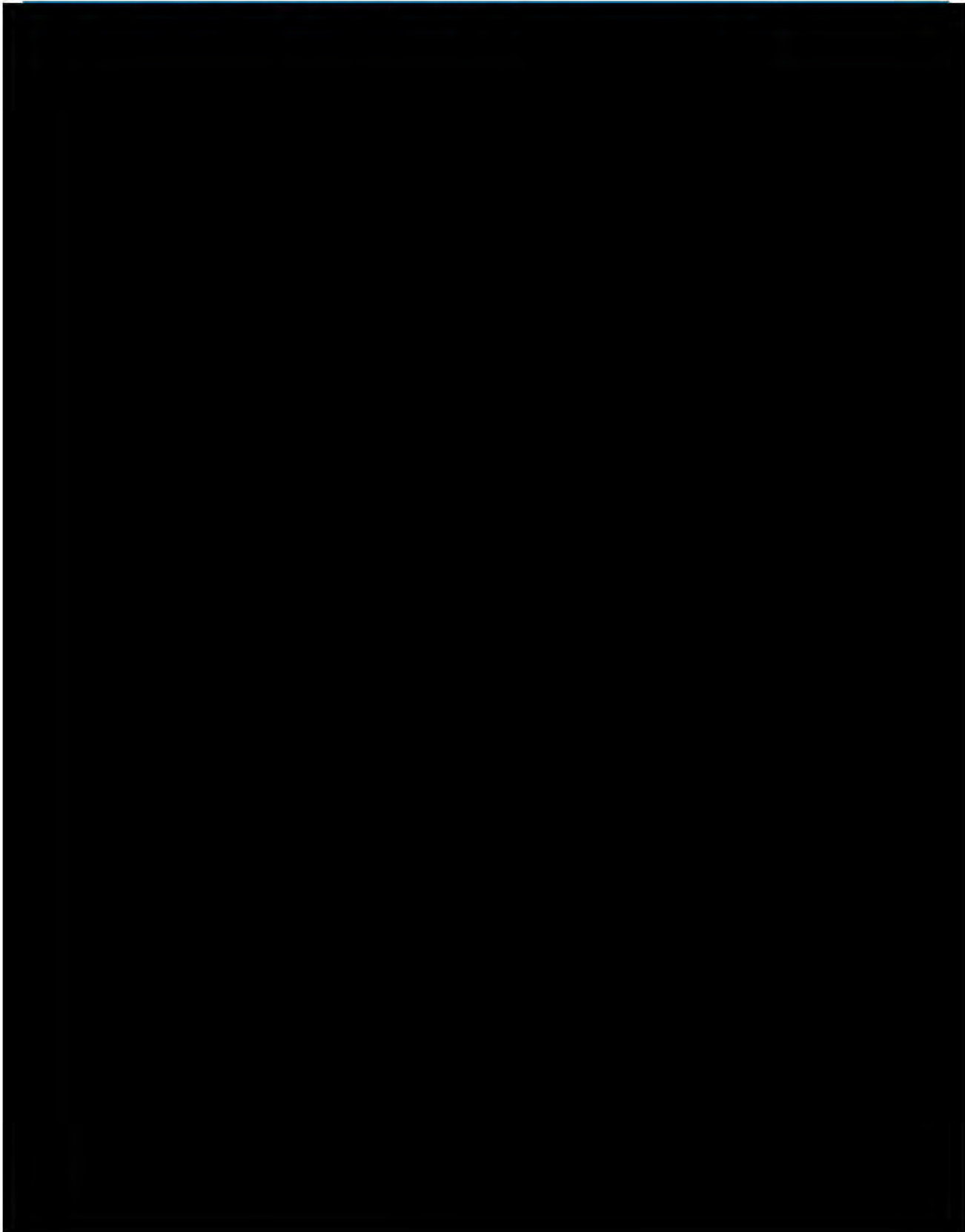
Table D-7.1-1. Commercial Fixed Satellite Service Verification Test Plan.

[illegible]

[illegible]

This image displays a complex geometric pattern, likely a digital artwork or a design element. It features a dense arrangement of rectangular and square shapes in various colors, including shades of blue, black, white, and gray. The shapes are arranged in a non-repeating, abstract layout, creating a visually busy and layered composition. The overall effect is one of depth and complexity, with the different colored blocks interacting to form a rich, textured surface.





D-8 Service Area: Managed Service

D-8.1 EIS Test Plan for Managed Network Service (MANDATORY) [L.30.2.4; E.2.2]

Table D-8.1-1. Managed Network Service Verification Test Plan.

Managed Network Service	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	

Table D-8.1-2. Managed Network Service Access Speed.

Location	Speed	Service Order Number
TBD	DS-1	TBD
Parameters to be Measured	Demonstrate that awarded services are delivered based on KPIs and SLAs defined in RFP Section C.2.8.1. Performance metrics specified at the TO-level per RFP Section C.2.8.1.4.	
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above.	
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.8.1	
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure		
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in this test approach for all new services during the NS2020 EIS Contract and added to service-specific test plans.	
Testing Conditions [E.2.2.1]		
Requirement	Description	
Agency defines additional Testing in TO	As defined in the specific TO	
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.	
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing.	
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]		
Requirement	Description	
Service TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1	
Test Cases [E.2.2.3; C.2.8.1.4]		
Requirement	Description	
TS-02	Test as defined in RFP Section E.2.2.2.1	
Test Case #1 AT&T defined		
Test Data Sets Determined by AT&T [E.2.2.4]		

Managed Network Service	
Requirement	Description
Test Data Sets Determined by AT&T	Trouble ticket report data
Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All test results, acceptance, and standards compliance reporting defined in RFP Section E.2.2.5
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval
EIS Testing Report	Provided within 3 days of service installation and testing

D-8.2 EIS Test Plan for Web Conferencing Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-8.2-1. Web Conferencing Service Verification Test Plan.

Web Conferencing	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	
Parameters to be Measured	Demonstrate that awarded services are delivered based on KPIs and SLAs defined in RFP Section C.2.8.2.4.1
Measurement Procedure	Calculate availability for on a monthly basis and compare against the WCS AQL of $\geq 99.9\%$ based on events tracked by trouble tickets
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.8.2.4.1
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	If a test fails in any service verification test, appropriate service-specific remediation will take place, followed by re-testing.
Development of EIS Test Plan for all New Services during the Life of the Contract	
Testing Conditions [E.2.2.1]	
Requirement	Description
Testing Conditions	Business as usual for monthly operations and trouble ticket collection intervals
Agency Defines Additional Testing in TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing.
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]	
Requirement	Description

Web Conferencing	
Service TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1
Test Cases [E.2.2.3; C.2.8.2.4]	
Requirement	Description
TS-02 Test Case #1 AT&T defined	
Test Data Sets Determined by AT&T [E.2.2.4]	
Requirement	Description
Test Data Sets Determined by AT&T	
Test Results and Acceptance[E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All test results, acceptance, and FedRAMP and FISMA compliance reporting defined in RFP Section E.2.2.5
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval
EIS Testing Report	Provided within 3 days of service installation and testing

D-8.3 EIS Test Plan for Unified Communications Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-8.3-1. Unified Communications Service Verification Test Plan.

Unified Communications	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	

Table D-8.3-2.

Unified Communications		
Table D-8.3-2. Unified Communications Service Network Access Speed.		
Location	Speed	Service Order Number
Location 1	100Mbps	TBD subsequent to award
Parameters to be Measured	The following aggregate Key Performance Indicator (KPI), defined in RFP Section C.2.8.3.4.1 Performance Metrics of the EIS RFP, with exception to the measurements to be verified by the performance of the test cases described in other sections of this service specific test plan. ▪ Availability — Routine: ≥ 99.5%	
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology. See Test Methodology above.	
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.8.3.4.1	
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure		
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in this plan for all new services during the life of the NS2020 EIS Contract and added to service-specific test plans.	
Testing Conditions [E.2.2.1]		
Requirement	Description	
Agency Defines Additional Testing in TO [E.2.2.1]	As defined in the specific TO	
Observation of EIS services verification testing by government representatives [E.2.2.1]	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.	
AT&T to Provide all Test Equipment [E.2.2.1]	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing.	
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]		
Requirement	Description	
Service TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1	
Test Cases [E.2.2.3; C.2.8.3.4]		
Requirement	Description	
TS-02 Test Case #1 determined by AT&T	The UCS test plan defines one verification test case, listed in the table D-8.3.3.	

Unified Communications						
Table D-8.3-3. UCS Verification Test Cases.						
Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result	Actual Result
1	Availability - Routine	≥ 99.5%		30 days	≥ 99.5%	TBD
Test Data Sets Determined by AT&T [E.2.2.4]						
Requirement		Description				
Test Data Sets Determined by AT&T						
Test Results and Acceptance[E.2.2.5]						
Requirement		Description				
Test Results and Acceptance		All test results, acceptance, and FedRAMP and FISMA compliance reporting as defined in RFP Section E.2.2.5				
Deliverables [E.2.2.6]						
Requirement		Description				
EIS Test Plan		Provided for government approval				
EIS Testing Report		Provided within 3 days of service installation and testing				

D-8.4 EIS Test Plan for Managed Trusted Internet Protocol Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-8.4-1. Trusted Internet Protocol Service Verification Test Plan.

Managed Trusted Internet Protocol Service	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	

Table D-8.4-2.



Parameters to be Measured	The following aggregate KPIs for the Trusted Internet Connection (TIC) Portal, as defined in RFP Section C.2.8.4.4.1 of the EIS RFP, will be verified by the performance of the test cases described in this service specific test plan. ▪ Availability (TIC Portal) — Routine ▪ GOS (Failover Time) ▪ GOS (Monitoring and Correlation) — Routine ▪ GOS (Monitoring and Correlation) — Critical ▪ GOS (Configuration/ Rule Change) — Routine ▪ Event Notification (EN) (Firewall Security) ▪ EN (Intrusion Detection/ Prevention Security) ▪ GOS (Virus Updates and Bug Fixes) The following aggregate KPIs for the MTIPS Transport Collection and Distribution, as defined in RFP Section C.2.8.4.4.2 of the EIS RFP, will be
	verified by the performance of the test cases described in this service specific test plan as summarized in Table D-8.4.3. ▪ Availability (Port) — Routine ▪ Availability (Port) — Critical ▪ Latency (CONUS) — Routine ▪ Latency (CONUS) — Critical ▪ GOS (Data Delivery Rate) — Routine ▪ GOS (Data Delivery Rate) — Critical EN (Security Incident Reporting)



Managed Trusted Internet Protocol Service

Table D-8.4-3. MTIPS KPI Parameters to be Measured.

Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result	Actual Result
1	Availability (Port) — Routine					TBD
2	Availability (Port) — Critical					TBD
3	Latency (CONUS) — Routine					TBD
4	Latency (CONUS) — Critical					TBD
5	GOS (Data Delivery Rate) — Routine					TBD
6	GOS (Data Delivery Rate) — Critical					TBD
7	EN (Security Incident Reporting) — Routine					TBD

Measurement Procedure Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology above.

Acceptance (Pass/Fail) Criteria Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Sections C.2.8.4.4.1 and C.2.8.4.4.2.

Fallback approach to describe the fallback process and procedures in case of testing failure

Development of EIS Test Plan for all New Services during the Life of the Contract EIS test plans will be developed using the process in this plan for all new services during the life of the NS2020 EIS Contract and included service-specific test plans.

Testing Conditions [E.2.2.1]

Requirement	Description
Agency Defines Additional Testing in TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing.

Test Scenarios (scenarios selected per service requirement) [E.2.2.2]

Requirement	Description
Service TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1

Test Cases [E.2.2.3; C.2.8.4.4]

Requirement	Description
-------------	-------------

Managed Trusted Internet Protocol Service						
TS-02 Test Case #1 Determined by AT&T		Table D-8.4-4.				
Table D-8.4-4.MTIPS KPI Verification Test Cases. [C.2.8.4.4]						
Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result	Actual Result
1	Availability (TIC Portal) — Routine/Critical					TBD
2	GOS (Failover Time) — Routine					TBD
3	GOS (Monitoring and Correlation) — Routine					TBD
4	GOS (Monitoring and Correlation) — Critical					TBD
5	GOS (Configuration/ Rule Change) — Routine					TBD
6	EN (Firewall Security Event Notification) — Routine					TBD
7	EN (Firewall Security Event Notification) — Routine					TBD
8	EN (Firewall Security Event Notification) — Routine					TBD
9	EN (Intrusion Detection/ Prevention Security Event Notification) — Routine					TBD
10	EN (Intrusion Detection/ Prevention Security Event Notification) — Routine					TBD
11	GOS (Virus Protection Updates and Bug Fixes) — Routine					TBD
12	GOS (Virus Protection Updates and Bug Fixes) — Routine					TBD
Test Data Sets Determined by AT&T [E.2.2.4]						
Requirement		Description				

Managed Trusted Internet Protocol Service	
Test Data Sets Determined by AT&T	
Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All test results, acceptance, and FISMA compliance reporting as defined in RFP Section E.2.2.5
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval
EIS Testing Report	Provided within 3 days of service installation and testing

D-8.5 EIS Test Plan for Managed Security Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-8.5-1. Managed Security Service Verification Test Plan.

Managed Security	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	

Table D-8.5-2. MSS Services and Functions.

Location	Service/Function	Service Order Number
Location 1	Managed Prevention Service (MPS)	TBD subsequent to award
Location 2	Vulnerability Scanning Service	TBD subsequent to award
Location 3	Incident Response Service	TBD subsequent to award
MSS Testing Schedule. The Managed Security Service (MSS) availability performance data is continuously collected and recorded from the servers in the AT&T MSS network. As such, a testing schedule for availability is not required. Previous month averages will be available within the first few days of the new month. Monthly averages for event notification response times, incident response times, configuration change		defines the measurable KPIs between agency premise routers for an MSS. The following information provides the details on the MSS service order that is undergoing verification testing: ■ Service Order Number: This will be supplied after the agency places the order
times, and virus protection update times will be calculated for each month. Server availability and response times are measured by internal systems. No further resources are required to provide verification test data. RFP Section C.2.8.5.4.1		■ Service Locations Involved with Verification Testing: This involves the all of the POPs within the AT&T network involved with the transport for the MSS. Associated Access Arrangement Order Information: The Wireline Access Arrangement order information will be included with the service order information
Parameters to be Measured		The following aggregate KPIs, as defined in RFP Section C.2.8.5.4.1 Performance Metrics of the EIS RFP, will be measured. Exception to the measurements will be verified by the performance of the test cases described in other sections of this service-specific test plan.

Managed Security	
	▪ Availability – Routine  ▪ EN — Routine for MPS ▪ EN — Routine for Incident Response Service (INRS) ▪ GOS — Routing (Configuration Change, Virus Updates) ▪ Incident Response Time (Telephone) Routine — Low Category Incident ▪ Incident Response Time (Telephone) Routine — High Category Incident ▪ Incident Response Time (On Site) Routine — Low Category Incident ▪ Incident Response Time (On Site) Routine — High Category Incident
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.8.5.4.1
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in this plan for all new services during the life of the NS2020 EIS Contract and added to service-specific test plans.
Testing Conditions [E.2.2.1]	
Requirement	Description
Agency Defines Additional Testing in the TO	As defined in the specific TO
Observation of EIS Services Verification Testing by Government Representatives	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing.
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]	
Requirement	Description
Service TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1
Test Cases [E.2.2.3; C.2.8.5.4]	
Requirement	Description
TS-02 Test Case #1 Determined by AT&T	

Table D-8.5-3. MSS Verification Test Cases. [C.2.8.5.4.1]

Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result	Actual Result
1	Availability — Routine					TBD
2	Availability (Port) – Routine for TICS (see Note 1)					TBD
3	Availability (Port) – Critical for TICS (See Note 1)					TBD
4	Latency – Routine for TICS (See Note 2)					TBD
5	Latency – Critical for TICS (See Note 2)					TBD
6	GOS (Data Delivery Rate) – Routine for TICS (See Note 3)					TBD
7	GOS (Data Delivery Rate) – Critical for TICS (See Note 3)					TBD
8	EN Security Incident Reporting – for TICS (See Note 4)					TBD
9	EN for MPS - Routine					TBD
10	ENs for INRS — Routine — Low Category Event					TBD
11	ENs for INRS — Routine — Medium Category Event					TBD
12	ENs for INRS — Routine — High Category Event					TBD
13	GOS (Configuration Change, Virus Protection Updates) — Routine — Normal Priority					TBD
14	GOS (Configuration Change, Virus Protection Updates) — Routine — Urgent Priority					TBD
15	Incident Response Time (Telephone) — Routine — Low Category Incident					TBD
16	Incident Response Time (Telephone) —					TBD

Managed Security						
	Routine — High Category Incident					
17	Incident Response Time (On Site) — Routine — Low Category Incident					TBD
18	Incident Response Time (On Site) — Routine — High Category Incident					TBD

D-8.6 EIS Test Plan for Managed Mobility Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-8.6-1. Managed Mobility Service Verification Test Plan.

Managed Mobility Service	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for the service.

Managed Mobility Service	
Test Methodology	
MMS Testing Schedule	The MMS availability performance data is continuously collected and recorded from the servers in the AT&T MMS network. As such, a testing schedule for availability is not required. Previous month averages will be available within the first few days of the new month. Monthly averages for EN response times, incident response times, configuration change times, and virus protection update times will be calculated for each month. RFP Section C.2.8.6.4.1 defines the measurable KPIs between agency premise routers for an MMS. ▪ MMS Verification Testing Resources. Server availability and response times are measured by internal systems. No further resources are required to provide verification test data. The following information provides the details on the MMS service order that is undergoing verification testing. ▪ Service Order Number: This will be supplied after agency places the order ▪ Service Locations Involved with Verification Testing: This involves all of the POPs within the AT&T network involved with the transport for the MMS. ▪ Associated Access Arrangement Order Information: The Wireline Access Arrangement order information will be included with the service order information
Parameters to be Measured	The following aggregate KPIs, as defined in RFP Section C.2.8.6.4.1 Performance Metrics of the EIS RFP, will be measured. Exception to the measurements will be verified by the performance of the test cases described other sections of this service specific test plan. ▪ Event Notification — Routine ▪ Grade of Service — Routine (Configuration Change) ▪ Incident Response Time (Telephone) — Routine ▪ Incident Response Time (Dispatch) — Routine
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.8.6.4.1
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in this plan for all new services during the life of the NS2020 EIS Contract and added to service-specific test plans.
Testing Conditions [E.2.2.1]	
Requirement	Description
Agency Defines Additional Testing in the TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T.
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing.
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]	

Managed Mobility Service	
Requirement	Description
Service TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1
Test Cases [E.2.2.3; C.2.8.6.4]	
Requirement	Description
TS-02 Test Cases determined by AT&T	Table D-8.6-3

Table D-8.6-2. MMS Verification Test Cases. [C.2.8.6.4.1]

Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result	Actual Result
1	Event Notification (EN) Routine					TBD
						TBD
						TBD
2	Grade of Service (Configuration Change)					TBD
						TBD
3	Telephone Incident Response Time					TBD
						TBD
4	Dispatch Incident Response Time					TBD
						TBD
5	Availability					TBD

Test Data Sets Determined by AT&T [E.2.2.4]	
Requirement	Description
Test Data Sets Determined by AT&T	

Managed Mobility Service	
Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All test results, acceptance, and FedRAMP and FISMA compliance reporting per RFP Section E.2.2.5
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval
EIS Testing Report	Provided within 3 days of service installation and testing
D-8.7 EIS Test Plan for Audio Conferencing Service (OPTIONAL) [L.30.2.4; E.2.2]	
Table D-8.7-1. Table Audio Conferencing Service Verification Test Plan.	
Audio Conferencing Service	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	
Parameters to be Measured	The following two aggregate KPIs, as defined in RFP Section C.2.8.7.4 of the EIS RFP, will be verified: ▪ Availability (Av) ▪ Grade of Service (GOS): Operator Assistance Response Delay
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service and TO requirements. See Test Methodology above.
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs defined in RFP Section C.2.8.7.4
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in this plan for all new services during the life of the NS2020 EIS Contract and added to service-specific test plans
Testing Conditions [E.2.2.1]	
Requirement	Description
Agency Defines Additional Testing in TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]	

Managed Mobility Service						
Requirement		Description				
Service TS-02 [E.2.2.2.1; G.8]		Test as defined in RFP Section E.2.2.2.1				
Test Cases [E.2.2.3; C.2.8.7.4]						
Requirement		Description				
TS-02 Test Cases determined by AT&T						
Table D-8.7-2. ACS Verification Test Cases.						
Test Case	KPI	AQL	Test Case Description	Test Period	Acceptable Result ¹	Actual Result
1	Availability (Av) — Routine					TBD
2	GOS Operator Assistance Response Delay — Routine					TBD
¹An "Acceptable Result" occurs when each test case result falls within the calculated allowance for routine availability. This calculation is derived using the following formula: Av is calculated as a percentage of the total reporting interval time that the ACS is operationally available to the agency. Availability is computed by the standard formula: $Av(IDPS) = RI(HR) - COT(HR) \times 100RI(HR)$ Grade of Service (GOS) is measured based on the following formula: $GOS = \frac{Number\ of\ Blocked}{(Number\ of\ Offered\ Calls)}$ To perform this test, we will query our call data collection and reporting systems for the quantities of offered and blocked calls on existing government networks. The data used will be from the first full month immediately preceding the test date.						
Test Data Sets Determined by AT&T [E.2.2.4]						
Requirement		Description				
Test Data Sets Determined by AT&T						
Test Results and Acceptance [E.2.2.5]						
Requirement		Description				
Test Results and Acceptance		All test results, acceptance, and standards compliance reporting as defined in RFP Section E.2.2.5				
Deliverables [E.2.2.6]						
Requirement		Description				
EIS Test Plan		Provided for government approval				
EIS Testing Report		Provided within 3 days of service installation and testing				

D-8.8 EIS Test Plan for Video Teleconferencing Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-8.8-1.

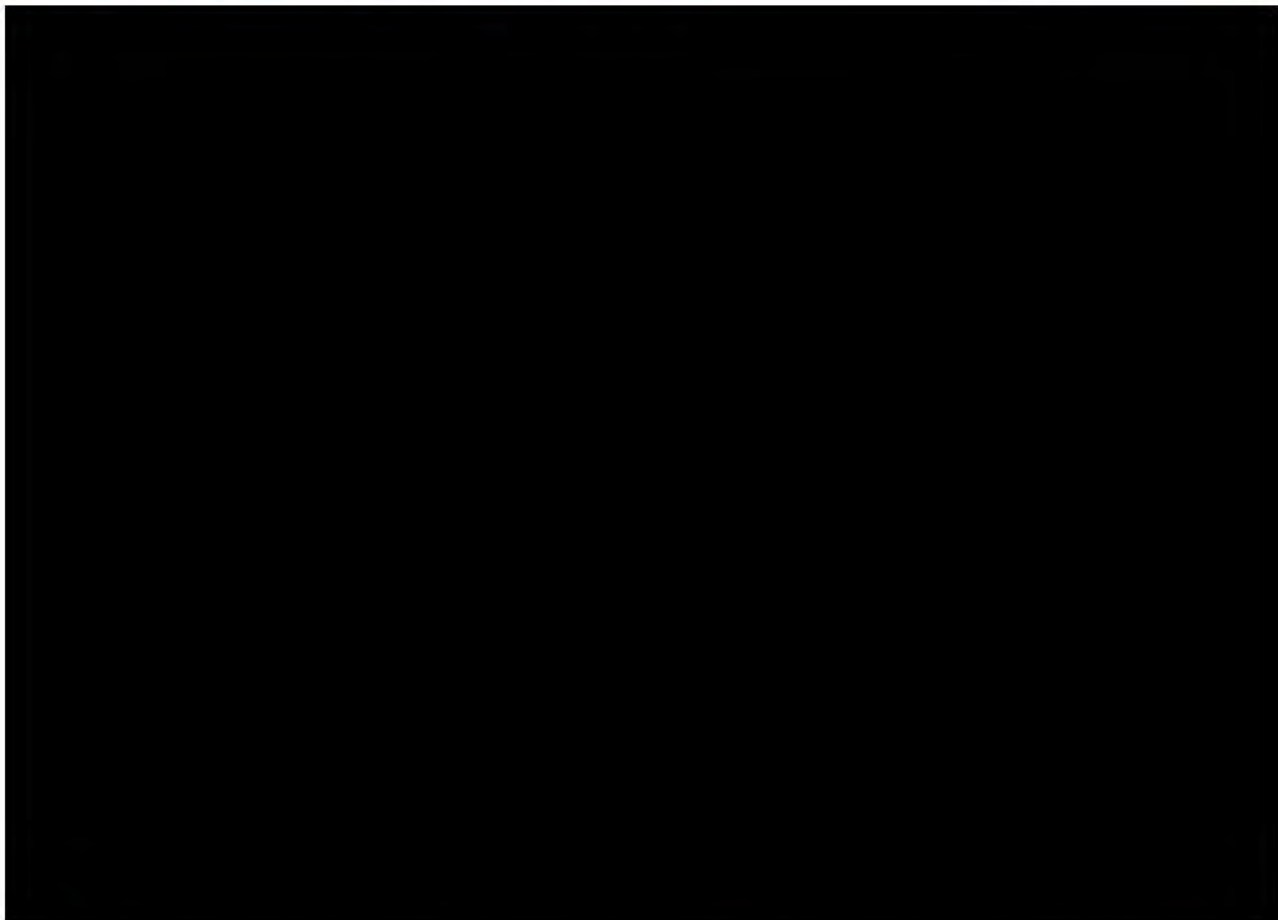
[REDACTED]

[REDACTED]

Test Scenarios (scenarios selected per service requirement) [E.2.2.2]	
Requirement	Description

[REDACTED]

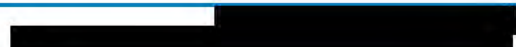
[REDACTED]



D-8.9 EIS Test Plan for DHS Intrusion Prevention Security Service (OPTIONAL) **[L.30.2.4; E.2.2]**

Table D-8.9-1. DHS Intrusion Detection Service Verification Test Plan.

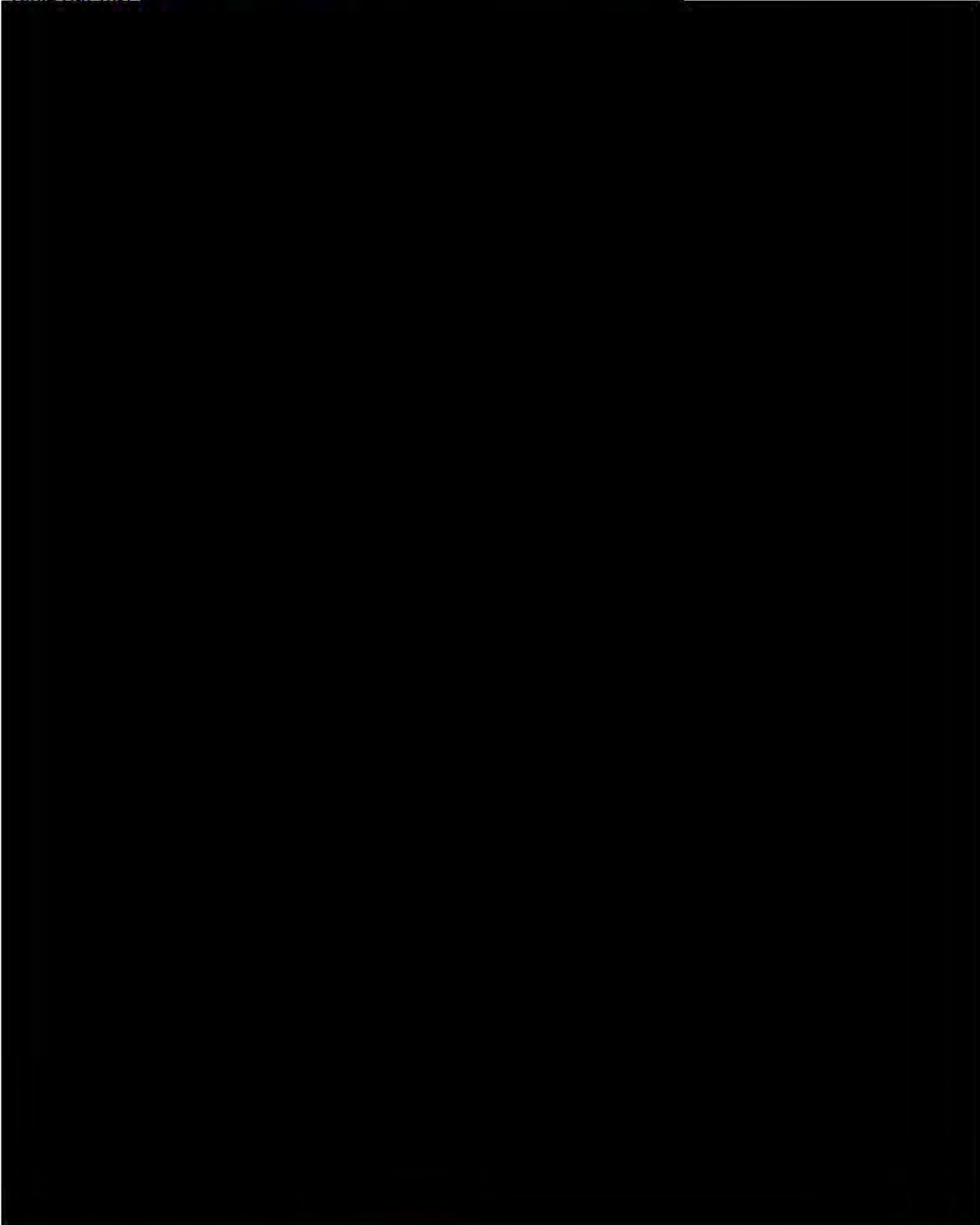
DHS Intrusion Prevention Security Service	
General Testing Requirements [E.2.2.1]	
Requirement	Description
Verification and Acceptance Testing Approach for all Awarded EIS Services	Verification and acceptance testing will be performed specific to the KPIs, AQLs, and SLAs of each type of this service using processes in this table and assumptions in Appendix D introduction. Acceptance testing will be defined in the TO for IPSS.
Development of EIS Test Plan	Each service will have a verification test plan that demonstrates compliance with the KPIs for that service.
Test Methodology	
Parameters to be Measured	To be defined in the TO
Measurement Procedure	Measurement procedure(s) will be implemented in support of and in accordance with steps in the service test methodology process for this service using the TO requirements. See Test Methodology above
Acceptance (Pass/Fail) Criteria	Documented demonstration that service works properly according to KPIs and AQLs as defined in the TO



DHS Intrusion Prevention Security Service	
Fallback Approach, to Describe the Fallback Process and Procedures in Case of Testing Failure	
Development of EIS Test Plan for all New Services during the Life of the Contract	EIS test plans will be developed using the process in this plan for all new services during the life of the NS2020 EIS Contract and added to specific test plans
Testing Conditions [E.2.2.1]	
Requirement	Description
Agency Defines Additional Testing in the TO	As defined in the specific TO
Government Representatives Can Observe all or Any Part of EIS Services Verification Testing	EIS verification testing will accommodate observation by government representatives, upon notice to AT&T
AT&T to Provide all Test Equipment	AT&T provides all test equipment, hardware, software, and analysis tools for all service testing
Test Scenarios (scenarios selected per service requirement) [E.2.2.2]	
Requirement	Description
Service TS-02 [E.2.2.2.1; G.8]	Test as defined in RFP Section E.2.2.2.1 and defined in the TO
Test Cases [E.2.2.3; C.2.8.9.4]	
Requirement	Description
TS-02 Test Cases Determined by AT&T	Test cases will be defined at the time of service by AT&T to address the requirements in the Agency Task Order.
Test Data Sets Determined by AT&T [E.2.2.4; E.2.2]	
Requirement	Description
Test Data Sets Determined by AT&T	
Test Results and Acceptance [E.2.2.5]	
Requirement	Description
Test Results and Acceptance	All test results, acceptance and compliance reporting as defined in RFP Section E.2.2.5
Deliverables [E.2.2.6]	
Requirement	Description
EIS Test Plan	Provided for government approval
EIS Testing Report	Provided within 3 days of service installation and testing

D-8.10 EIS Test Plan for Software Defined Wide Area Network Service (OPTIONAL) [L.30.2.4; E.2.2]

Table D-8.10-1



D-9 Service Area: Access Arrangements [C.1.8.1] (MANDATORY COMPONENT)

D-9.1 EIS Test Plan for Access Arrangements [L.30.2.4; E.2.2]

Per RFP Section C.2.9, AT&T has determined that testing for access arrangements, as a standalone service is not applicable. Access arrangements will be treated as a component of EIS transport services. Thus, Verification Testing and SLA reporting will be per each specific service.

D-10 Service Area: Service Related Equipment [C.1.8.1]

D-10.1 EIS Test Plan for Service Related Equipment (OPTIONAL) [L.30.2.4; E.2.2]

AT&T has determined that testing is not applicable to this service.

D-11 Service Area: Service Related Labor [C.1.8.1]

D-11.1 EIS Test Plan for Service Related Labor [L.30.2.4; E.2.2]

AT&T has determined that testing is not applicable to this service.

D-12 Service Area: Cable and Wiring [C.1.8.1]

D-12.1 EIS Test Plan for Cable and Wiring [L.30.2.4; E.2.2]

AT&T has determined that testing is not applicable to this service; however, AT&T will verify EIS cable and wiring installations are installed per TO specifications. If the TO



has no specifications, AT&T will verify EIS cable and wiring installations are in installed accordance in AT&T specifications for that type of installation.



General Services Administration (GSA)

Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

GS00Q17NSD3000

Appendix E — Climate Risk Management Plan

APPENDIX E — CLIMATE RISK MANAGEMENT PLAN [L.30; L.30.2.5; M.2.2 (4 OF 7); G.12]

Introduction: This appendix is AT&T's response to RFP requirements contained in RFP Section G.12 of the EIS solicitation, "Requirements for Climate Change Adaptation, Sustainability, and Green Initiatives." **Appendix E** also contains our initial Climate Risk Management Plan, responsive to the EIS RFP Deliverable Table F.2.1, deliverable #84, Corporate Climate Risk Management Plan, due with proposal submission. AT&T already conducts extensive corporate sustainability reporting both on our corporate website and through accredited, widely recognized third parties. All our sustainability reporting is regularly updated and posted to our websites, both corporate and third party. **Section E-1.d** below, provides additional detail of our corporate sustainability reporting. RFP Section G.12.1 enumerates the requirements and content required for a Plan that complies with federal government policy articulated in Executive Order (EO) 13693. The White House issued Executive Order 13693 Planning for Federal Sustainability on March 19, 2015 to maintain U.S. leadership in sustainability and greenhouse gas emission reduction. We assert the policy applicable to United States federal government agencies — and by extension, contractors — "that agencies shall increase efficiency and improve their environmental performance."

This appendix describes our commitment to sustainability and corporate citizenship, and how these tenets are woven into corporate and executive leadership structures, written into company policy, and made available publicly on corporate websites and in conjunction with 3rd party entities. In addition, this appendix contains the Climate Risk Management Plan itself, describing how AT&T will comply with EO 13693, contractual requirements, and applicable federal, state, and local laws and directives. The plan aligns to RFP Sections G.12.1 and G.12.2 and addresses how climate risk planning is incorporated into our overall EIS risk process. AT&T understands that sustainability related standards, lifecycle cost estimates, and environment impacts of proposed solutions apply at the EIS contractual and Task Order (TO) level as well as the EIS contractual levels.

AT&T Leadership in Sustainability and Corporate Responsibility: Sustainability is a way of doing business at AT&T. Our approach recognizes our company's effect on

society and the environment, and acknowledges that a company of our size, scope, and resources has a unique responsibility to lead and set an example for others to follow on environmental and social issues.

Our commitment is built into the executive leadership and governance structures. The AT&T Board of Directors includes a Public Policy and Corporate Reputation Committee, which exercises oversight over all Citizenship and Sustainability (C&S), issues, including environmental sustainability and the management of company Greenhouse Gas (GHG) emissions. Our executive leadership team includes a Chief Sustainability Officer who coordinates sustainability initiatives firm-wide and reports to the Public Policy Committee. At the executive level, our Citizenship and Sustainability (C&S) Steering Committee is made of senior AT&T executives and officers with responsibility for business areas most linked to sustainability priorities. The committee meets quarterly to identify priorities and align resources. It is led by the Chief Sustainability Officer, who works with the Chairman's office, Board of Directors and the executive management team to integrate sustainable business practices across the company and its supply chain. Within C&S, multiple skilled teams focus on individual sustainability issues. For instance, the Corporate Real Estate Energy Team calculates GHG emissions. Another cross-functional team directs strategy and communication. The Energy Council manages emissions: its director is empowered to manage efforts across business units, driving programs to reduce energy use and directing AT&T energy purchasing strategies.

Our commitment is also written into formal company policy. The AT&T Climate Change Policy and Energy Policy are publicly available on our Corporate Social Responsibility website (www.att.com/csr), a link to which will be included on the AT&T EIS website (www.att.com/gov/eis). As of October 2015, AT&T was one of 81 companies signed to the American Business Act on Climate pledge, a White House initiative for companies to curb greenhouse gas emissions and invest in clean energy.

Recognizing that one company is limited in the effect it can make, AT&T collaborates with peers, clients, and third parties to promote Information and Communications Technology (ICT) solutions that deliver economic, social, and environmental benefits. To this end, we participate in and work through organizations to publicly promote the

use of technology to address climate and resource challenges, including the Global e-Sustainability Initiative (GeSI), the Digital Energy and Sustainability Solutions Campaign (DESSC), Green Grid, the Alliance for Telecommunication Industry Solutions, the BlueGreen Alliance, the Business Roundtable, CDP, Carbon War Room and GreenBiz.

Climate Risk Management Plan: Climate Risk Management Planning is incorporated into AT&T risk management programs, including the EIS Risk Management approach discussed in the Program Management Plan (Section A-8) as well as in the AT&T corporate risk management framework, and is an ongoing part of our risk management and risk mitigation strategy for EIS. Climate change adaptation aspects have been carefully considered and incorporated into the design and operations of services to be provided under the EIS contract.

Moreover, this appendix constitutes our initial Climate Risk Management Plan (RFP Deliverable Table F.2.1, #84), and contains two distinct elements: Climate Change [G.12.1]. Adaptation and Sustainability and Green Initiatives [G.12.2]. Taken together, these elements comply with applicable sections of EO 13693, as well as with all EIS contractual requirements, and with applicable federal, state, and local laws and directives. Our EIS Climate Risk Management Plan will be regularly updated and the most current version will be available for GSA's use in supporting their own adaptation plans.

E-1 Climate Change Adaptation [G.12.1]

Part One of the AT&T Climate Risk Plan for EIS incorporates climate change adaptation strategies into our formal risk-management programs to reduce risk to company real estate, infrastructure, and supply chain operations. Section 13 of EO 13693 articulates the policy governing climate adaptation, preparedness, and resilience to be followed by federal agencies.

Executive Order 13693

Section 13. Supporting Federal Facility Climate Preparedness and Resilience. The head of each agency shall...ensure that agency operations and facilities prepare for impacts of climate change...by:

- (a) Identifying and addressing projected impacts of climate change on mission critical water, energy, communication, and transportation demands and considering those climate impacts in operational preparedness planning for major agency facilities and operations...

E-1.a — Climate Risk Adaptation and Risk Planning: AT&T performs a formal sustainability strategic assessment to identify key risks and opportunities. This assessment includes identification of mission critical facilities, products and services, an evaluation of business operations and supply chains that may be vulnerable, and a process of anticipating needs arising from climate change. Based on this assessment, AT&T incorporates climate change adaptation strategies into the design and operations of services to be provided under EIS.

AT&T is the first company in the nation certified under the Department of Homeland Security (DHS) “Private Sector Preparedness Program” (PS-Prep™), certifying that AT&T can maintain or recover its own business operations when disaster strikes. The PS-Prep™ program helps us better plan for, respond to, and recover from disasters and threats, and is part of our readiness plan for the potential of climate-related events. In the event of climate related, natural, or man-made disasters, AT&T is prepared to maintain its network and services, to support affected communities, and provide assistance to victims through network preparedness, network response and technology, employee action, and corporate giving.

The AT&T Weather Operations Center monitors potential nature-related threats to our network, employees, and communities. These exercises and the Weather Operations Center help enable us to minimize damages and mobilize our response even faster. We monitor and maintain our networks 24/7 and conduct several readiness drills throughout the year to help confirm that our networks and personnel are prepared to respond quickly. When disaster strikes, our employees work around the clock to keep the network up and running. The Network Disaster Recovery (NDR) team has more than 30 permanent members in the United States and the United Kingdom, with more than 100 volunteer members in the United States and abroad who have other full-time jobs in AT&T.

Critically, AT&T also makes products and services available to assist governments when disaster strikes. These situations often require collaboration in state and local government sectors to help agencies across geographies to maintain understanding of local, state, and national news and events. Identified risks and opportunities are shared across company operations and categorized by individual business units.

At the corporate level, the Chief Sustainability Officer presents results from annual materiality assessments to the C&S Steering Committee and to the Board of Directors. This guides corporate decisions on programs, investments, goals, and reporting. At an asset level, our corporate real estate, risk management, external affairs, and business continuity teams all play a role in assessing these risks. They monitor legislation that might affect energy prices, for example. They also track energy use in a centralized database in real-time, which illuminates areas with potential risks and/or opportunity. Energy use and natural disasters are two of the most substantial risks and opportunities for AT&T at an asset level. To further mitigate risk at an asset level, a cross-functional team from the corporate real estate, network, IT, and other related organizations uses a proprietary site selection methodology that includes characteristics such as exposure to natural disasters (flood and drought zones) and expected electricity and water availability and costs to determine site locations.

AT&T is committed to keeping our customers connected — even in the wake of climate-related, unpredictable, or catastrophic events — by maintaining the reliability of the AT&T global network. The mission of the NDR Team is to recover AT&T voice and data service network elements to an area affected by a disaster. AT&T has invested more than \$600 million in its U.S. NDR program and another \$15 million internationally. Telecommunications is vital for our business and government customers following a disaster, for the affected area and for the rest of the country. AT&T launched its NDR program in 1992 to provide a way to rapidly restore network services after a catastrophic disaster. We post detailed information about the AT&T NDR program on our public corporate website, www.corp.att.com/ndr.

To assess climate-related risk to our operations, we use the AT&T Climate Change Analysis Tool (CCAT). Developed with the U.S. Dept. of Energy's Argonne National Labs, CCAT allows us to visualize and identify the location of infrastructure at risk for physical climate-related impacts, including sea level rise. CCAT helps us anticipate potential impacts of climate change on our network infrastructure and business operations up to 30 years into the future by combining Argonne's regional climate modeling data with sophisticated mapping capabilities and allows us to visualize climate

change risk on company infrastructure and make climate-informed decisions for the future.

E-1.b — Transparency and Reporting: Transparency and accountability are critical elements of our Climate Risk Management Plan that we achieve through public reporting and participation in third party surveys and audits. AT&T posts its own corporate performance against sustainability and GHG reduction goals to our public corporate website. All sustainability disclosures are timely and kept up to date. These sites will be linked to the EIS website as well. Additionally, we participate in numerous third party surveys of corporate sustainability and responsibility, and link to those reports within our own public websites. Public reporting is a critical element of our Climate Risk Management Plan.

E-1.c — Accredited Third Party Reporting: AT&T updates sustainability disclosures annually. AT&T uses recognized third-party sustainability reporting portals and services to publish the results of our sustainable efforts. Some of these reports and reporting portals include:

- **Global Reporting Initiative (GRI):** Our reporting efforts are aligned to the GRI internationally accepted sustainability reporting framework.
- **CDP Climate Change Response:** We have submitted disclosure to CDP since 2005 and will continue to report to CDP on an annual basis.
- **Sustainability Disclosure Database (Database of Corporate Social Responsibility (CSR) Reports):** Each year, we issue an annual sustainability update to summarize our work from the past year, capture progress toward our goals, review key performance indicators, and discuss our present and anticipated opportunities and challenges.

Trucost (Accredited Third Party): AT&T conducts annual corporate sustainability reporting, backed by Trucost, an accredited third party. Results are published and accessible to GSA and the public on our website. Trucost's rigor around this process helps AT&T confirm accuracy in reporting metrics.

E-1.d — Sustainability Disclosures and Reporting: Under EIS, the Customer Service Office (CSO) will prepare an annual Climate Change Adaptation, Sustainability, and

Green Initiatives Report (F.2.1 Deliverable 85) detailing changes made during the year to remain compliant with EO 13693 requirements, and cataloging products used which are covered by the EnergyStar, Federal Energy Management Program (FEMP), and Electronic Product Environmental Assessment Tool (EPEAT) Programs. The EIS Climate Change Adaptation, Sustainability, and Green Initiatives Report includes an annual summary of corporate sustainability efforts in the past calendar year and captures progress toward those goals and key performance indicators. In any situation, the EIS Program Manager (PM) will notify the GSA CO or any affected agency in a timely manner if conditions arise that are out of compliance with the EO, laws, regulations, or directives.

AT&T works to reduce our environmental influence with the same passion and leadership we bring to all aspects of our business. AT&T established policies and initiatives in a number of areas including: Eco-Rated devices, Water Management, Energy Reduction, Device Recycling, Transportation Initiatives, Paper Management and Supply Chain.

E-2 Sustainability and Green Initiatives [G.12.2]

AT&T provides sustainable products and services whenever possible, including sustainable acquisition and data center requirements of EO

13693, including the use of Energy Star-certified low standby power, or EPEAT-registered products. When offered, AT&T identifies, by model, which products offered are Energy Star qualified/certified, meet FEMP low standby power levels, and/or EPEAT-registered, with EPEAT-registered products broken out by registration level of bronze, silver, or gold. AT&T established sustainability goals and commenced corporate investments in climate-related and GHG reduction initiatives before EO 13693 or its predecessor orders were issued. Section 2 of the EO states the federal government goals for GHG reduction. AT&T is committed to comply with climate change adaptation conditions described in EO 13693, other EOs, laws, regulations and directives specified in the EIS RFP.

As part of our ongoing commitment to sustainability and climate resiliency, AT&T has established a number of goals dedicated to managing and reducing our environmental footprint in several key categories, including greenhouse gas emissions, energy, water, and waste management, and corporate fleet and transportation. As we near or reach attainment of our 2020 and 2025 goals, we're setting our sights even higher — identifying new measures that continue to push us and reflect the direction of our evolving business.

Technology companies are in a unique position to help customers — from individuals to large enterprises and government organizations — mitigate their environmental effect and improve their climate resiliency. Information and Communication Technology (ICT) solutions from AT&T, comprising hardware, software, and broadband and wireless technologies, can enable people and businesses to make more energy-efficient choices and reduce environmental effect. Attaining a competitive advantage drives our sustainability efforts. By reducing energy use — our primary source of emissions — we can reduce associated costs, which ultimately benefit our bottom line. Being more resilient to natural disasters and enabling continuity of operations makes our service more attractive to our customers. Communicating with consumers about how our services allow them to operate more sustainably offers a competitive advantage.

Public goals have long-guided our work. We have set our goals with this question in mind: how can we work with our customers, our employees, our suppliers, and our communities to enhance the world we all share? Our long-term goals help us target our resources and keep us accountable for progress. We are not just focused on outputs, but on outcome and our influence. Our goals are focused on three distinct areas of our business: our network and customers, our supply chain, and our community.

E-2.a — Corporate Climate Change Considerations: The AT&T Climate Change Policy states our belief that the ability to increase resource efficiency and reduce greenhouse gas (GHG) emissions will be a primary determinant of success in the 21st century world economy. Technology plays a critical role in empowering the transition to

the low-carbon economy, better managing resource use, and increasing business resiliency. We work with industries, governments, nonprofits, and academia to promote technology that tackles climate and resource challenges.

AT&T continually takes steps to confirm our company's resiliency in the face of volatile weather and resource scarcity. We disclose this information in our annual submission to the CDP Climate Change Response survey.

Table E-2-1 summarizes our stances, actions, and positions on several key areas and results AT&T is focused on in relation to climate resiliency, business operations, and environmental effect.

Table E-2-1. AT&T Leadership in Sustainability. AT&T Positions and Actions on Climate Change Considerations.

Climate Change Consideration	AT&T Position
Energy Use	We take action to reduce energy consumption from non-renewable sources and to source portions of our energy from renewable sources. We approach this in 3 ways: - Invest: Purchasing large-scale renewable energy contracts that deliver clean energy to local grids and reduce our overall Scope 2 emissions - Reduce and right-size: Eliminating unnecessary load by both removing power from unnecessary assets and properly diminishing capacity commensurate with the demand placed on AT&T services - Optimize: Incorporating energy-efficient systems, products, methods and practices into building infrastructure and monitoring the holistic operation and energy performance of buildings and systems to identify and address energy-impacting maintenance deficiencies and opportunities In 2020, we invested more than \$100 million to implement approximately 8,800 projects that amount to gross annualized savings of \$40 million. Since 2010, we have implemented nearly 147,000 energy efficiency projects, resulting in annualized energy savings of nearly 7.6 billion kWh and cost savings of \$694 million.
Greenhouse Gas Emissions	We've been measuring and disclosing our GHG emissions annually since 2008. In 2020, we committed to reaching carbon neutrality by 2035 across our entire global operation. We will achieve net zero Scope 1 and 2 emissions³ through steps such as accelerating network optimization and energy efficiency projects, virtualizing many network functions, expanding sustainable media production, and scaling our renewable energy use. Our goals are to: - Achieve carbon neutrality (net zero Scope 1 and 2 GHG emissions) by 2035 - Reduce our absolute Scope 1 and Scope 2 GHG emissions 63% by 2030, (against the 2015 baseline). - Work to ensure that 50% of our suppliers (covering purchased goods and services, capital goods and downstream leased assets as a portion of spend) set their own science-based Scope 1 and Scope 2 targets by 2024.

Climate Change Consideration	AT&T Position
Company Fleet & Transportation	Directly addressing fleet-related emissions, To reduce fleet emissions, we are exploring several opportunities, including electrifying our fleet. In early 2020, we joined the Corporate Electric Vehicles Alliance (CEVA), which serves as a platform for companies to collaborate to increase corporate demand for electric vehicles (EVs). Through our membership in CEVA, we can work with other companies to identify challenges and opportunities involved in adding EVs to our fleet.. By the end of 2020, AT&T reduced U.S. ground fleet emissions by 332,658 metric tons of CO₂e or 38.4% from our 2008 baseline. In addition to reducing the size of our domestic fleet by more than 8 thousand vehicles, 81% of passenger sedans procured for our domestic fleet since 2010 were hybrid vehicles. Optimizing our fleet operations is also a crucial component to making real changes. We use leading practices to efficiently manage our fleet every day, including use of fleet management technology solutions, and we continue to explore new ways to reduce fuel use and drive fewer miles.
Water	Water is important to the communities where we operate and to our own operations. The network that forms the core of our business requires a controlled and cooled environment, and water is often a critical input to the cooling equipment we use. We exceeded our goal to reduce AT&T's water consumption relative to data growth on our network 60% by 2020 (using a 2013 baseline) a year ahead of schedule. In 2020, we further reduced our water consumption by 11% compared to 2019. And, in 2021, we launched a new goal to reflect our commitment to using critical water resources efficiently. By 2030, we aim to achieve a 15% reduction (2019 base year) in U.S. water use in high- or extremely high-water stress areas.
Disaster Response	To better understand how AT&T is positioned to respond to climate change, we assess the potential impacts and the magnitude of climate-related risks on our operations, including network infrastructure, our products, the company and our brand. Our new Climate Change Analysis Tool helps us visualize climate change risk on our infrastructure and make smarter, climate-informed decisions. Instead of relying on 10-day weather forecasts and historic events, we can now model climate-related phenomena like projected sea-level rise and the potential impact on surrounding cables, cell sites or data centers – decades into the future. These insights can help us better plan for maintenance, construction and disaster recovery efforts as we serve our customers and communities. We are also adapting our business practices to adjust to the realities of climate change, including in weather and natural disaster patterns. To maintain the reliability of our network and keep our customers connected, AT&T has cell site standards that apply across our entire operating area. Those standards meet the requirements in all relevant jurisdictions but will often exceed what may be required in some individual geographies. We conduct regular analysis to help ensure our cell sites can withstand natural disasters and other environmental factors. We also deploy high-capacity battery backup to our cell sites, which allows them to remain in service in the event of a power loss. To prepare our network for natural disasters, we regularly test the batteries located at every site and take steps to ensure any fixed generators are fueled on a regular basis.
Supply Chain	Suppliers are a key part of our business and therefore must be part of our approach to sustainability and diversity. We have suppliers around the world (in non-embargoed countries) representing all types of trades, engaged across all our operating units. AT&T Communications works with more than 20,000 suppliers

Climate Change Consideration	AT&T Position
	around the world. The reach of our supply chain allows AT&T the opportunity to streamline operations, reduce long-term costs and limit overall environment impact. Our top supply chain goals are: 2024 Science Based Target: Work to ensure 50% of our suppliers (covering purchased goods and services, capital goods, and downstream leased assets as a portion of spend) set their own science-based Scope 1 and Scope 2 GHG targets. 2025 Goal: Help establish clear, agreed-upon industry sustainability metrics to measure the environmental and social impact of technology supply chains. Promote the use of sustainability metrics in industry sourcing. Develop and follow an industry roadmap toward truly sustainable performance among our suppliers.

E-2.b — Sustainable Management Practices: The previous section articulates AT&T corporate commitment to sustainability. Sustainability and sustainable practices flow all the way to how we manage our engagements. The EIS PM and agency customer executives are committed to complying with applicable environmental, health and safety laws and regulations, and to maintaining and improving management systems throughout the company to meet our compliance obligations. AT&T has a team of highly qualified personnel with experience to comply with sustainability related requirements including the following: Project Managers, Management Leadership, Sustainability Office, Public Policy Committee of the Board of Directors, and a Citizenship & Sustainability Steering Committee. **Table E-2-2** summarizes AT&T internal management practices used in our Climate Risk Management Plan approach:

Table E-2-2. AT&T Leading Sustainability Through Action. *AT&T works to meet sustainability goals with specific actions and measurable goals.*

AT&T Practices	Description
EcoSpace	Makes it easier for GSA agencies to purchase devices based on sustainability. Devices are rated based on five environmental and social considerations: - Environmentally preferred materials - Minimization of substances of concern - Energy efficiency - Responsible end of life treatment and recycling - Environmentally and socially responsible manufacturing - Eco-Rating 2.0 considers 20 performance criteria, including environmentally and socially responsible manufacturing factors, and includes cell phones, tablets, and accessories
Climate Action	AT&T explores both mitigation and adaptation strategies when considering climate change risks. We take action to reduce our energy consumption and strive to increase the amount of renewable electricity in our portfolio.

AT&T Practices	Description
	As part of our previous commitment to purchase more than 1.5 gigawatts (GW) of renewable energy capacity domestically, in 2020 we announced agreements representing more than 500 megawatts (MW) of solar energy – making AT&T one of the largest corporate purchasers of solar energy in the world. To help build our resilience and adapt to climate change AT&T has engaged the U.S. Department of Energy's Argonne National Laboratory for help assessing the risks of climate change to our business. This is the first such project publicly announced in the telecommunications industry and brings together insights from the laboratory's regional climate modeling data with the sophisticated mapping capabilities of AT&T data scientists. This effort led AT&T to develop a Climate Change Analysis Tool (CCAT) that helps anticipate potential impacts of climate change on our infrastructure and operations.
Water Management	Since 2013, when we set our first water goals, we have taken action resulting in water savings of 6 billion gallons. By 2030, we aim to achieve a 15% reduction (2019 base year) in U.S. water use in high- or extremely high-water stress areas.
Energy	We take action to reduce energy consumption from non-renewable sources and to source portions of our energy from renewable sources. We approach this in 3 ways: • Invest: Purchasing large-scale renewable energy contracts that deliver clean energy to local grids and reduce our overall Scope 2 emissions • Reduce and right-size: Eliminating unnecessary load by both removing power from unnecessary assets and properly diminishing capacity commensurate with the demand placed on AT&T services • Optimize: Incorporating energy-efficient systems, products, methods and practices into building infrastructure and monitoring the holistic operation and energy performance of buildings and systems to identify and address energy-impacting maintenance deficiencies and opportunities
Transportation	By the end of 2020, AT&T reduced U.S. ground fleet emissions by 332,658 metric tons of CO₂e or 38.4% from our 2008 baseline. In addition to reducing the size of our domestic fleet by more than 8 thousand vehicles, 81% of passenger sedans procured for our domestic fleet since 2019 are hybrid vehicles.
Device Recycling	AT&T proactively seeks to create productive uses for our waste at the end of its life. In total, AT&T managed 200,000 metric tons (MT) of waste and recovered more than 24 million consumer devices in 2020.
Supply Chain	■ Work with AT&T suppliers to improve energy use, greenhouse emissions, hazardous substances, water, packaging, waste and end-of-life recycling. ■ Approaches include: – Strategic Supplier Sustainability Scorecard – Reducing packaging materials – Supplier sustainability awards annually honoring suppliers that make outstanding contribution to sustainability.

E.2.c — Sustainability Initiatives: AT&T has initiatives in place to confirm we have a resource efficient future ahead to serve our customers. Our carbon neutral goal shows our commitment to reduce our own emissions as well as delivering solutions that help our customers achieve their net zero ambitions. AT&T is committed to providing ICT

solutions that improve business operations and the potential to reduce environmental effect. Several of our AT&T technical solutions feature environmental and social benefits, including:

- **Energy and Building Management System:** Monitor and reduce energy usage in your facilities - from offices to factories - by collecting equipment performance data into a single system that alerts if energy is being wasted.
- **Asset Management:** Track stationary or mobile assets to prevent loss, reduce inspection and maintenance trips and optimize energy efficiency.
- **Unified Communications (UC):** By improving the organization's ability to have productive remote and flex workers, AT&T UC services can help reduce the need for local commuting and fixed office space and their associated environmental costs and effects.
- **Telepresence:** An AT&T-sponsored study by Carbon Disclosure Project (CDP) and Verdantix found that by 2020, U.S. businesses with revenues of more than \$1 billion can collectively achieve financial benefits of almost \$15 billion and reduce CO2 emissions by nearly 4.6 million metric tons by substituting Telepresence meetings for some business travel.
- **Cloud Computing:** Using the cloud removes the need to store anything on hardware devices and associated data centers that require large amounts of electricity to power and cool facilities. AT&T found that by 2020, large U.S. companies that use cloud computing can achieve annual energy savings of \$12.3 billion and annual carbon reductions equivalent to 200 million barrels of oil, which is enough to power 5.7 million cars for one year.
- **Data Centers:** Section 3 of EO 13693 states sustainability goals for data centers. AT&T uses the most efficient data centers and cloud services available compliant with Power Utilization Efficiency (PUE) requirements, whether on our own network, or provided by third-party vendors.
- **Fleet Management:** Smarter transportation tackles inefficiencies by reducing fuel consumption through automated route planning. These technologies can also increase vehicle efficiency through the reduction of idle time, better management of

miles driven, adherence to speed rules, monitoring of vehicle acceleration, and other strategies. The resulting efficiency gains can deliver fleet-wide performance improvements that can lead to reduced energy waste and reduced greenhouse gas emissions. Along with our business alliance members, we offer many vehicle-based solutions that combine the latest advances in Global Positioning Systems (GPS), wireless, and web technologies to make mobile workforce and fleet management a more affordable reality.

E-2.1 Electronic Product Environmental Assessment Tool [G.12.2.1]

For TOs that include requirements for AT&T to purchase electronic equipment on behalf of government clients under EIS for use by agency employees or on their facilities, EIS uses Electronic Product Environmental Assessment Tool (EPEAT) registered products level bronze or higher. Specific products used are subject to TO requirements and agency needs. AT&T is committed to conducting business with the highest standard of integrity and ethics and with abiding respect for corporate citizenship and sustainability. Suppliers are an important part of our business and therefore must be an important part of our approach to citizenship and sustainability. To this end, the EIS takes advantage of corporate policies and procedures in place as well as infrastructure employed specifically to vet products procured on behalf of the government, provided for government use, or used on federally controlled facilities to confirm it registered at the EPEAT bronze, silver, or gold levels.

E-2.2 Energy Efficient Products [G.12.2.2]

Section 3 of Executive Order 13693 articulates the following sustainability goals for use of Energy Star and Federal Energy Management Program products for agencies.

Similarly, EIS uses existing policy, procedure, and corporate infrastructure in the use or procurement of energy-consuming products procured and provided for use by the government, or used on government facilities to comply with

Executive Order 13693

Section 3. Sustainability Goals for Agencies. The head of each agency shall....:

- (i) Promote sustainable acquisition and procurement by ensuring...the following environmental performance and sustainability factors are included to the maximum extent practicable...
- (B) Energy and water efficient products and services, such as ENERGY STAR qualified and Federal Energy Management Program (FEMP)-designated products, identified by EPA and the Department of Energy (DOE).

energy efficiency requirements, (e.g., EnergyStar certified, or Federal Energy Management Program (FEMP)-designated products) in accordance with FAR Clause 52.223-15 Energy Efficiency in Energy-Consuming Products. As described earlier, the EIS CSO will prepare and deliver a Climate Change Adaptation, Sustainability, and GHG Reduction Initiatives report annually to the GSA CO (F.2.1 #85) enumerating products (as appropriate) by model number that meet Federal Energy Management Program (FEMP), EnergyStar, and EPEAT standards.

Specific products and models of routers, switches, and hosting/storage/power equipment used will be determined by requirements detailed in individual TOs. To the extent AT&T purchases or procures power-consuming electronic equipment for use by the government or on government facilities — including routers, switches, and hosting/storage/power equipment — EIS opts to offer EnergyStar certified, low standby power products, or EPEAT registered products level bronze or higher.

E-2.2.a — Sustainable Supply Chain: All of our model supply chain-managed material and services agreements contain a standard Citizenship and Sustainability clause that requires the suppliers to align with the AT&T Principles of Conduct for Suppliers, and to respond to sustainability-related information requests from AT&T. The clause is standard in all new master agreements as of 2011; AT&T has executed thousands of agreements that contain the clause. We also have several clauses in our contract library that cover sustainability considerations such as energy efficiency. We continue to work with our major network suppliers to establish goals to improve the efficiencies of next-generation network equipment and we work with the Alliance for Telecommunications Industry Solutions (ATIS) on using the Telecommunications Energy Efficiency Ratio (TEER) metric. We are already seeing results collaborating with strategic network suppliers with TEER baselines and goals in our agreements.

AT&T expects suppliers to apply a continuous improvement approach to enhance economic, social, and environmental conditions.

We expect suppliers to add value through innovative products and services, elimination of wasteful practices, increased energy efficiency, reduced total cost of ownership, reduced

greenhouse gas emissions, more sustainable packaging, reduced water use, and end-of-life recycling alternatives. Suppliers should implement procedures that reduce the environmental effect of their products and services. AT&T expects suppliers to minimize or eliminate the use of hazardous substances in products that we buy. We train more than 200 sourcing contract managers about sustainability in the supply chain and we are providing the tools necessary to engage our strategic suppliers on sustainable business practices.

E-2.3 Data Centers and Cloud Services [G.12.2.3]

AT&T helps businesses build and operate their IT infrastructure, which lowers the cost and effect of IT for businesses. Current trends toward cloud computing, server and storage virtualization, and low-energy cooling as a means to replace less-efficient data centers and application services have great potential to increase IT and data center efficiency.

Section 3 of Executive Order 13693 articulates sustainability goals for data centers. In accordance with EIS requirements, the Program Manager will deliver to GSA a Power Utilization Efficiencies (PUE) Report (F.2.1 Deliverable 86) upon delivery of our first TO response, with updates annually thereafter. Determinations about which data centers and cloud services to use on EIS are dependent upon TO-specific requirements, with individual centers and their PUE characteristics to be identified in responses to EIS TOs. In all cases, AT&T uses the most efficient data centers and cloud services available compliant with PUE requirements, whether on our own network, or provided by third party vendors.

Executive Order 13693

Section 3. Sustainability Goals for Agencies. The head of each agency shall... (ii) Improve data center energy efficiency at agency facilities by... (C) [e]stablishing a power usage effectiveness (PUE) target of 1.2 to 1.4 for new data centers and less than 1.5 for existing data centers.

Conclusion: AT&T is committed to corporate citizenship and sustainability. It is written into our policies and procedures and framed into our governance structures at the executive and Board of Directors levels. This commitment extends across all AT&T service solutions, and to individual contracts. Under EIS, this Climate Risk Management Plan presents our approach to plan for, and mitigate against, the effects of climate-change related events. This includes a plan that provides for climate risk adaptation

within our overall risk planning process, which identifies and engages specific sustainable practices, and which provides for regular and public reporting on our activity. This plan, to be updated annually under EIS, provides a means to drive preparedness, proactive engagement, public accountability, and transparency in reporting of our approach to climate change and sustainability. We do all this to provide GSA and government agencies confidence that our network is reliable and prepared for contingencies of all types, and that AT&T is doing its part as a corporate partner and responsible citizen to minimize our effect on the environment.



General Services Administration (GSA)

Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

GS00Q17NSD3000

Appendix F — Financial Status Report (Sample)

APPENDIX F — FINANCIAL STATUS REPORT (SAMPLE) [L.30; L.30.2.6; M.2.2(5 OF 7); G.9.5]

In order to track financial performance and growth across the EIS program, a view into total billing by customer and service is helpful. AT&T builds on experience providing GSA with accurate and timely financial status reports in support of both Networkx

Did You Know?

Demonstrated Performance and Reliability: As of submission of this EIS proposal, GSA has accepted 100% of Monthly Financial Status Reports submitted by AT&T since December 2007 under the Networkx contracts.

contracts to create the Financial Status Report in support of EIS. The EIS Financial Status Report complies with contractual requirements enumerated in RFP Section G.9.5 Financial Management and is broken down by service type, according to the Pricing Identification Structure in **Table B.1.2.1.1** of the EIS RFP. The list of service types and services will be updated as needed when additional services are added to the contract or if services are removed.

The EIS Financial Status Report will be provided in Excel format. The file will consist of two tabs: Summary and Detail.

- The Summary tab will contain a view summarized by service. The sample format of the Summary tab in AT&T's EIS Financial Status Report appears in **Figure F-1**.
- The Detail tab will provide a breakdown of billing by task order, agency, and service. The sample format of the Detail tab in AT&T's EIS Financial Status Report appears in **Figure F-2**.

This will be submitted as contractual deliverable F.2.1 #80 to the GSA PMO on the 15th of each month.

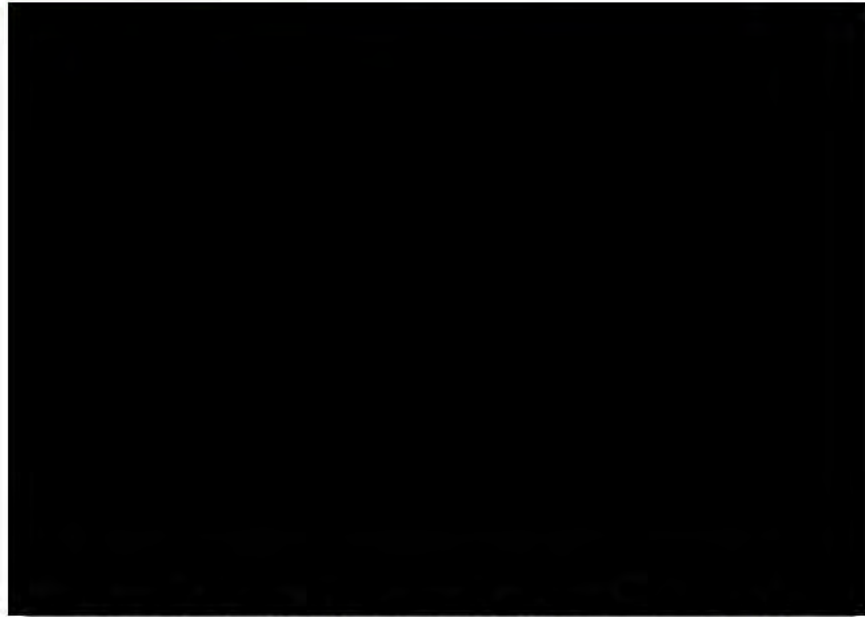


Figure F-1. Sample EIS Financial Status Report, Summary tab.

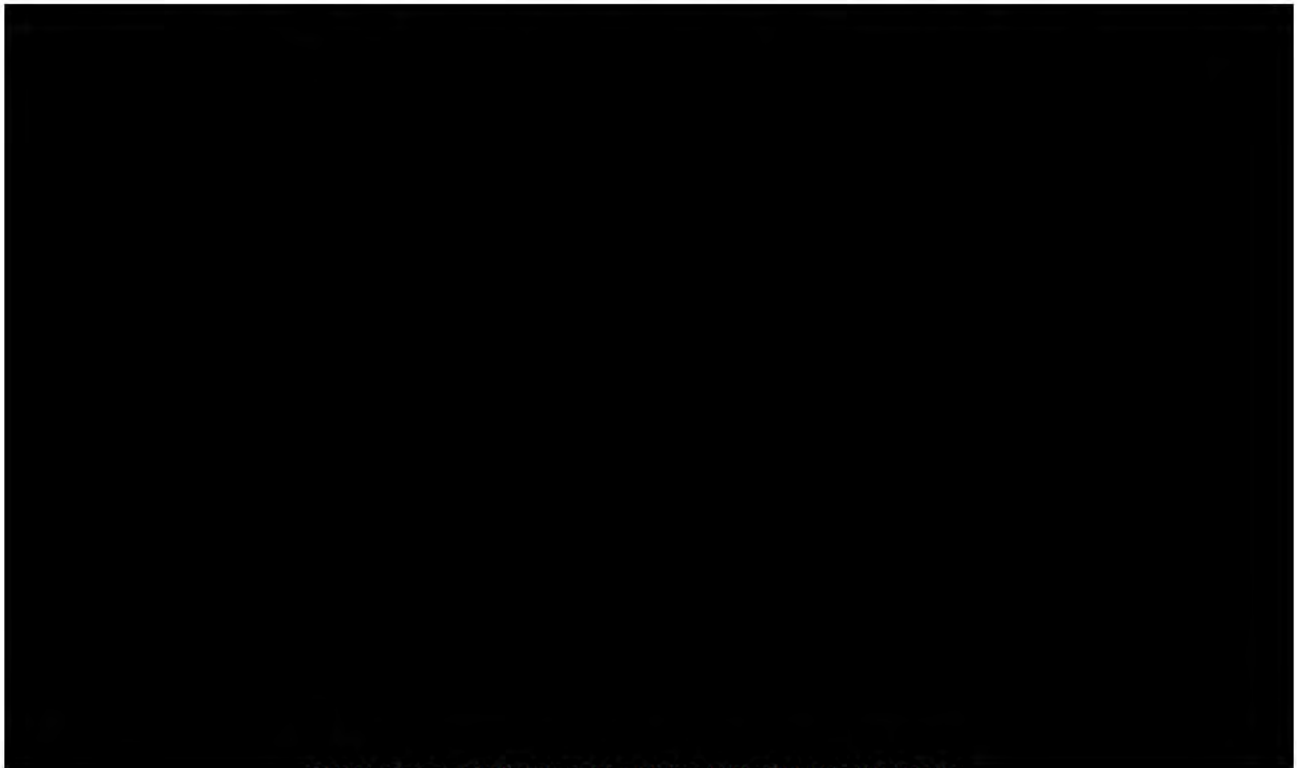


Figure F-2. Sample EIS Financial Status Report, Detail tab.



General Services Administration (GSA)

Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

GS00Q17NSD3000

Appendix G — BSS Risk Management Framework Plan

APPENDIX G — BUSINESS SUPPORT SYSTEMS (BSS) RISK MANAGEMENT FRAMEWORK PLAN [L.30; L.27.2; L.30.2.7; M.2.2.7; G.5.6; G.5.6.4; (2, 2A)]

As shown in **Figure G-1**, the Risk Management Framework (RMF) overlays the standard system development life cycle phases — Initiate, Design, Implement, Operations & Maintenance, and Dispose. The purpose is to integrate information security controls and activities throughout the life cycle in order to provide information systems with sufficient, risk-based, and ongoing security. **Appendix G** is AT&T's plan for applying the RMF to the BSS in compliance with the applicable regulations, policies, and guidance.

Per RFP Section L.11, AT&T will maintain the risk assessment for our BSS in accordance with the security authorization requirements in FAR Clauses 552-239-70 (Information Technology Security Plan and Security Authorization (Jun 2011) and -71 (Security Requirements for Unclassified Information Technology Resources).

G-1 General Security Compliance Requirements [G.5.6.1]

In applying the RMF to the BSS, we will comply with all references listed in RFP Section G.5.6.1. We will also comply with the current applicable federal and agency-specific IT security directives, standards, policies, and reporting requirements as referenced in the following sections, including making available any documentation, physical access, and logical access needed to support this requirement.

G-2 GSA Security Compliance Requirements [G.5.6.2]

We select, implement, assess, and monitor ongoing compliance with the applicable baseline security requirements specified in NIST Special Publication 800-53, rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for Moderate impact systems and the related GSA directives and guides. Our plan follows the guidance in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, issued February 2010, as described in the following subsections.

G-3 Security Assessment and Authorization (Security A&A) [G.5.6.3]

We complete the initial BSS Assessment and Authorization (A&A) before the BSS goes into production and begins processing Government information. Further, we maintain

the A&A through the continuous monitoring process, with a new security A&A conducted at least every 3 years or sooner if there is a significant system change that affects BSS' information security posture.

Our A&A approach is based 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 BSS and document the security categorization in the system security plan (SSP). GSA determined the security category of the BSS and the information that it will store, process, and/or transmit to be Moderate impact in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.
2. Describe the BSS, including system boundary, in the SSP.
3. Register the BSS with appropriate organizational program/management offices.
4. Identify any common controls that are inherited from systems outside the BSS's authorization boundary and document them in the SSP.
5. Select the BSS' security controls from the NIST 800-53, rev 4, baseline for a Moderate impact system and any additional controls required by GSA and/or needed to address specific information security risks and document them in the SSP.
6. Develop a continuous monitoring strategy for monitoring security control effectiveness and any proposed/actual changes to the BSS and its operating environment. The BSS continuous monitoring strategy reflects and is consistent with the GSA organizational continuous monitoring strategy and program as described in GSA's IT Security Procedural Guide: *Information Security Continuous Monitoring Strategy*, CIO-IT Security-12-66.
7. Submit the BSS SSP to the Authorizing Official (AO) for review and approval.
8. Implement the security controls specified in the SSP.
9. Document 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.

10. Develop a Security Assessment Plan (SAP) for testing the BSS to verify that the required controls specified in the approved SSP are implemented as described and providing the appropriate level of risk management. We submit the SAP to the AO or their designee for review and approval.
11. Execute the SAP to assess the BSS' security controls.
12. Prepare a security assessment report (SAR) to document any issues, findings, and recommendations from the security control assessment.
13. Conduct initial remediation actions based on the findings and recommendations in the SAR 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. As discussed in greater detail in RFP Section G-17, *Plan of Action and Milestones*, the Government determines the risk rating (critical/high, moderate, or low); we provide monthly updates on the status of any critical and high vulnerabilities that have not been resolved within 30 days.
15. Assemble the security authorization package and submit it to the AO for their authorization decision.

The basic authorization package consists of the following deliverables:

- SSP
- SAR
- POA&M

If the BSS inherits common controls, then we include either the authorization package for the common controls or a reference to that documentation. If any inherited common controls are provided by an external provider, we collect and provide to the AO the information needed to make the BSS' authorization decision.

We also include with the authorization package the additional documentation specified in the RFP Sections G and/or J, as follows and discussed individually in the sections below.

- Any applicable Interconnection Security Agreements (ISAs)
- Control Tailoring Workbook

- A GSA NIST SP 800-53, rev 4, Control Summary Table
- Rules of Behavior (RoB)
- System Inventory
- 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 appropriate
- Code Review Report, as appropriate.

Based on their review of the authorization package, the AO determines the level of risk that the BSS 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).

After the AO grants the BSS its ATO, the system moves into RMF Step 6, Monitor Security Controls, as discussed in more detail in RFP Section G-4.16, *Continuous Monitoring of Security Controls of AT&T's System with a Continuous Monitoring Plan*. At a summary level, our on-going security monitoring activities consist of the following:

- Assess the security impact of proposed or actual changes to the BSS and its operating environment.
- Assess a subset of the BSS' security controls consistent with the continuous monitoring plan.
- Remediate vulnerabilities based on the results of the ongoing monitoring activities and risk assessment, as prescribed and tracked through the POA&M.
- Maintain the SSP, SAR, and POA&M.
- Prepare and submit ongoing system security status reports to the AO as required by this RFP and the BSS continuous monitoring plan.

Based on the ongoing assessments and reporting, the AO continually determines whether BSS' risk level continues to be acceptable.

G-4 BSS System Security Plan (SSP) [G.5.6.4]

The purpose of the SSP is to document system-identifying information; individuals responsible for the plan and its execution; security-relevant information about the system, including its security requirements; and, most importantly, the security controls that are implemented and/or planned to address the system's security requirements. The SSP includes appendices such as a privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, incident response plan, and continuous monitoring strategy. These appendices serve multiple purposes, such as documenting bases for some of the control requirements (e.g., the privacy impact assessment); documenting inherited/common controls (e.g., system interconnection agreements), or supporting execution of some of the security controls (e.g., incident response plan).

Our approach to SSP development follows the guidance in NIST 800-18, rev 1, *Guide for Developing Security Plans for Federal Information Systems*. Specifically, we determine and document the following using the SSP template provided in NIST 800-18, rev 1:

1. The BSS' unique identifier and name.
2. The BSS' FIPS 199 categorization (MODERATE).
3. The BSS owner's name, title, agency, address, email address, and phone number.
4. The AO's name, title, agency, address, email address, and phone number.
5. Title, address, email address, and phone number of any other key personnel/other designated contacts.
6. The name, title, address, email address, and phone number of the person responsible for the BSS' system security.
7. BSS' operational status: Operational, Under Development, or Major Modification.
8. Information system type: major application or general support system.
9. BSS' function and purpose and their information processes.
10. A general description of the BSS technical system, including primary hardware, software, and communications equipment.

11. The following information about any systems that the BSS interconnect with:

- System name.
- Owning organization.
- System type (major application or general support system).
- Indication of whether there is an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or Memorandum of Agreement (MOA) of file.
- Date of the agreement, if in place.
- FIPS 199 category.
- A&A status.

12. Related laws, regulations, and policies that apply to the BSS' data security.

13. Minimum security controls selected for the BSS and how they are and/or will be implemented. This section is the core of the BSS SSP, reflecting the tasks of selecting the applicable controls from NIST SP 800-53, rev 4; tailoring them as necessary, and identifying any inherited common controls. For each control, we identify the control by title and number; describe how the control has been or will be implemented; describe how and why we apply any scoping guidance; and, for any common controls, identify who is responsible for its implementation.

14. SSP completion and approval dates.

We develop and submit the initial BSS SSP within 30 days of the NTP. Thereafter we update the SSP as needed through the continuous monitoring process described in RFP Section G-4.16, with updates when changes to the SSP elements occur, but at least annually. We also develop and submit the SSP appendices described in the following sections.

G-4.1 Security Assessment Boundary and Scope Document (BSD) [G.5.6.4(1)]

The security assessment Boundary and Scope Document (BSD) documents the information technology resources that constitute the system and therefore the system's security assessment and accreditation boundary. These comprise the devices and connectivity dedicated to the system, but not systems that are otherwise accredited.

The purpose is to establish and communicate the scope of the system environment that must be secured and of any interconnections with systems outside the boundary.

Our approach to developing the BSD aligns with the guidance in NIST SP 800-37, rev 1, and follows the GSA-provided template. At a summary level, our BSD includes the following:

- BSD document purpose.
- BSS general description, including the system's function and purpose, user organizations, type(s) of information and processing that the BSS provides, and each BSS module and its function.
- BSS security categorization, determined by GSA to be Moderate impact.
- BSS technical environment, including the name and description of the BSS' software, how the users access the BSS, and technical details of the general support system on which the BSS resides.
- Hardware/software matrix in the format shown in **Table G-4.1-1**.

Table G-4.1-1. Sample BSS Hardware/Software Matrix. *GSA Receives Clear Documentation of Boundary and Scope for BSS System to be Secured.*

Hardware Component	Location(s)	Operating System, Version	Database(s), Version(s)	Software, Version(s)	Function/Supported Module(s)

- Interconnection/information sharing description of planned or existing BSS interconnections/interfaces and connections with other systems.
- Proposed BSS A&A scope.
- A table that summarizes BSS' technical environment, consisting hardware comprising the production and development/test environments and the backup site.
- A table documenting the version and date of BSS' security artifacts, such as the SSP, Interconnection Security Agreement(s), Privacy Impact Assessment, Contingency Plan, and other security documents discussed in this plan.
- **Appendix A** — System Diagram
- **Appendix B** — Input/Output Diagram

We develop and submit the BSS BSD within 15 days of the NTP.

G-4.2 Interconnect Security Agreements [G.5.6.4(2)]

Dedicated connectivity between the BSS and any other information system must be authorized through an ISA that documents how the connection is accomplished, security requirements for the connectivity, and the type and sensitivity of the information

communicated. Developing ISAs includes assessing any risk introduced via the interconnection, identifying the security controls needed to mitigate or eliminate identified risk, and providing assurances that the needed controls are in place.

Our approach to developing ISAs follows the guidance in NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, and consists of the steps summarized in **Figure G-4.2-1** and described following the figure.

1. Establish a Joint Planning Team that includes both management and technical personnel responsible for both interconnecting systems. Those individuals are responsible for identifying all technical, information security, and administrative issues related to the connectivity; resolving any related issues; and drafting the ISA. The team continues to interact throughout the life of the interconnection to address and resolve any related issues that may arise.
2. Define a business case that addresses costs and benefits of the proposed interconnectivity as well as any potential risks — technical risks, for example, as well as information security risks. At this step, the Joint Planning Team agrees on the method for data exchange or transfer and on data protection steps — as well as both parties' commitment to protect the data. We include those agreements with the draft ISA.
3. Verify that system(s) with which BSS is interconnecting has a current ATO. The owner of the interconnecting system requires the same assurance, which can be provided once the BSS ATO is awarded.
4. Determine interconnection requirements such as the hardware and software requirements; information services that are needed over the interconnection, such as e-mail, file transfer protocol, RADIUS, Kerberos, database query, or file query; data sensitivity and related security controls that are required; and incident monitoring and

**Figure G-4.2-1. AT&T's
Interconnection Security
Agreement Process.**

response procedures, including who, how, and when to notify in case of a suspected incident.

5. Complete the ISA, including a description of the interconnection, with a topological drawing; technical and security requirements for the interconnection throughout its life cycle — set up, operation, and maintenance; and the agreed-upon security controls.
6. If agreeable to both ISA parties, responsible parties representing both sign and date the ISA.

We include any required ISAs with the initial A&A package, then review, update as needed, and submit annually.

G-4.3 Control Tailoring Workbook [G.5.6.4(3)]

The purpose of the Control Tailoring Workbook is to document any AT&T control settings/assignments that differ from GSA-specified settings and our planned EIS control settings/assignments for which GSA allows contractor deviation. For example, GSA might specify that systems must off-load audit records onto a different system or media semi-annually, whereas we may require off-loading quarterly in compliance with our AT&T Security Policy & Requirements (ASPR). Therefore, we document planned/recommended deviations in column E of the Control Tailoring Workbook, adapting the provided template for NIST SP 800-53, rev 4.

We include the completed BSS Control Tailoring Workbook with the initial A&A package.

G-4.4 GSA Control Summary Table for a Moderate Impact Baseline [G.5.6.4(4)]

The purpose of the Control Summary Table is to maintain an overview of the status of each required security control. We populate and maintain the Table by indicating the implementation status: Implemented, Partially Implemented, or Not Applicable for each required control. **Table G-4.4-1** is a sample of our Control Summary Table which is based on GSA's template.

Table G-4.4-1. Sample Control Summary Table. GSA receives a template-based, compliant, control summary table.

Control	Status	*System Specific	*Common	*Hybrid	Comments
AU-6 (1)					
AU-6 (3)					
AU-7					
AU-7 (1)					

Control	Status	*System Specific	*Common	*Hybrid	Comments
AU-8					
AU-8 (1)					

We validate and update the Table as necessary after each security assessment, when control status is tested.

We include the original Control Summary Table with the initial A&A package.

G-4.5 Rules of Behavior [G.5.6.4(5)]

The purpose of the Rules of Behavior (RoB) is to inform anyone granted BSS access of their responsibilities to protect the security of the system and Government data stored, processed, or transmitted by the BSS.

We develop and maintain a RoB document consistent with GSA IT Security Procedural Guide 06-30; GSA Order CIO 2104.1, *GSA IT General Rules of Behavior*; and NIST SP 800-53, rev 4, Control PL-4, Rules of Behavior. Specifically, we:

1. Develop, document, and distribute to individuals who require BSS access the rules that describe their responsibilities and expected behavior with regard to secure information and BSS use.
2. Require that each such individual within our control sign acknowledgment of the Rules, indicating that they have read, understood, and agree to abide by them. We do not authorize any user's BSS access until they have signed and returned the RoB.
3. Review and update the Rules as needed annually.
4. Require that individuals who signed a previous version read and re-sign when the Rules are revised/updated.

We include the BSS RoB with the initial A&A package and submit annual updates, as necessary, thereafter.

G-4.6 System Inventory [G.5.6.4(6)]

A complete and accurate inventory of system components is essential for tracking and reporting as well as for verifying that appropriate security controls are applied to all components within the accreditation boundary. Further, a system inventory that includes hardware, software, and related information is required for compliance with NIST SP 800-37 RMF guidance and GSA IT Security Procedural Guide 06-03. Therefore, we prepare a current inventory of all BSS system components that are within the system

security authorization boundary. We document the system components in sufficient detail to support tracking and reporting, such as hardware identifying information (device type, manufacturer, model, serial number, and location), software license information and version numbers, component owner(s), and, for networked components, data such as machine name and network address.

We include the BSS System Inventory with the initial security A&A package, with annual updates thereafter.

G-4.7 Contingency Plan [G.5.6.4(7)]

The purpose of this task is to develop, test, and maintain three interdependent and mutually-supporting plans that enable us to recover and restore BSS functionality in the event of a disruption. We use the results of the BIA discussed in RFP Section G-4.7.2 to guide the recovery requirements and priorities addressed in the CP. The DRP discussed in RFP Section G-4.7.1 integrates with the CP by planning procedures to relocate BSS operations to an alternate location if that should be necessary. The centerpiece plan, the CP, consists of the procedures and capabilities for recovering the BSS from any form of unavailability, whether resulting from compromise, natural events, or system failure of any kind.

Figure G-4.7-1 provides an overview of AT&T's contingency planning process.

Our approach to developing, integrating, and maintaining the CP follows the guidance in NIST SP 800-34, rev 1, *Contingency Planning Guide for Federal Information Systems*, to develop a BSS-specific plan that can be activated independent of any other plan, such as the DRP, or in concert with the DRP if the system's operations need to be relocated until fully restored. Specifically, we do the following:

- Develop the BSS CP that:
 - Reflects the results of the BIA, scaled to the BSS' essential mission and criticality
 - Identifies BSS' recovery objectives, restoration priorities, and metrics.
 - Describes contingency strategies — actions to be taken under likely disruption scenarios.
 - Specifies plan activation, execution, and maintenance roles, responsibilities, and contact information for management and the personnel who would activate the CP.

- Includes procedures and resources for continuing operations that depend on the BSS in case of a system disruption.
- Documents restoration procedures and resources.
- Test and revise the CP as discussed in RFP Section G-4.8.
- Once tested, reviewed, and approved, distribute to all stakeholders — BSS management and the individuals responsible for executing the CP.
- At least annually, review the CP for any system, operational, or other changes that require plan revisions.
- Distribute updated CP to all plan stakeholders.

Because the CP is likely to include sensitive system information, such as device identifiers and location(s), AT&T restricts access to the plan to those with a need to know.

We include the CP, with DRP and BIA, in the initial A&A package and, as updated, annually thereafter.

G-4.7.1 Disaster Recovery Plan (DRP) [G.5.6.4(7).1]

As noted in RFP Section G-4.7, the DRP integrates with the CP by describing procedures to be followed to relocate BSS operations to an alternate processing site if there were a major system disruption that is expected to have long-term effects on operation site availability.

Consistent with guidance in NIST SP 800-34, the BSS DRP addresses only system disruptions that require processing relocation to an alternate site. That is, our DRP specifies the following:

- The alternate site location and its provisions for providing alternate processing. As the BSS is a FIPS 199 Moderate impact system, a “warm site” is likely, with partially-equipped spaces that contain only the most essential system hardware, software, telecommunications, and power sources, depending on the criticality and priorities determined through the BIA.
- The circumstances under which processing would be transferred to an alternate site.
- Guidance for making the determination to relocate to the alternate processing site.
- The individuals responsible for making the determination to implement the DRP.

- A communications plan, with contact information, for everyone likely to be affected by the DR effort.
- Provisions, resources, and procedures for moving BSS processing to the alternate site.

Once the DRP is prepared, we test the plan as discussed in RFP Section G-4.8 and revise as necessary before distributing it to the stakeholders. We include the DRP, along with the CP and the BIA, with the initial A&A package and, as revised, annually thereafter.

G-4.7.2 Business Impact Assessment (BIA) [G.5.6.4(7).2]

The BIA is critical to contingency planning and the DRP. Our approach is to complete the BIA early in the CP process, as the BIA results drive the contingency planning requirements and priorities. Our approach consists of four steps, consistent with NIST 800-34 guidance.

1. Document the business processes that the BSS supports. This is a restatement of the system description in the SSP, elaborated to map all of the business processes with BSS system processes.
2. Identify and document the criticality of each business process, then assess and document the impact of a system disruption on those processes. The output of this step is the anticipated impact of a BSS outage on the business (or mission) at different time increments. For example, the impact might be minimal for the first 24 hours, but serious if extended beyond that. The result is a best-estimate of the maximum BSS downtime that could be tolerated without compromising the mission.
3. Identify and document the resources that are required for recovery within the allowable timeframe. The resources include, for example, the physical facilities, personnel, hardware, software, data, and telecommunications.
4. Determine and document the BSS recovery priorities, resources that need to be in place, and sequenced recovery activities.

We include the BIA with the CP and the DRP in the initial A&A package and, as revised, annually thereafter.

G-4.8 Contingency Plan Test Plan (CPTP) [G.5.6.4(8)]

The purpose of this task is to develop a CPTP consistent with GSA IT GSA IT Security Procedural Guide 06-29, *Contingency Planning Guide*. We develop a CPTP that enables us to identify and address plan deficiencies well before a contingency occurs. Our CP testing, reflected in the CPTP, helps us identify potential weaknesses in the plan, assess our readiness to execute the plan, and confirm the accuracy of each recovery procedure. The Test Plan includes test cases to assess plan components such as:

- Notification procedures
- System recovery on an alternate platform from backup media
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- Other plan testing where coordination is identified, such as continuity of operations plan (COOP) or business continuity plan (BCP) testing

In coordination with the Government, we determine the type of testing that is appropriate for the BSS' CP such as walk-through/tabletop exercises, parallel or full interrupt simulations, or comprehensive exercises, based on BSS' sensitivity and the BIA conclusions.

We deliver the BSS CPTP with the initial A&A package and annually thereafter.

G-4.9 Contingency Plan Test Report [G.5.6.4(9)]

The objective of this task is to determine the CP's effectiveness and to identify potential plan weaknesses to verify that it would be effective if it ever has to be executed.

Although titled as "Contingency Plan Test Report," the purpose of this task is broader, consisting of:

- Executing the CPTP
- Analyzing the CP test results for lessons learned and corrections that need to be made
- Correcting findings from the CPTP execution

- Documenting the test results in a Contingency Plan Test Report (CPTR) consistent with GSA IT Security Procedural Guide 06-29 guidance.

We deliver a BSS CPTR with the initial security A&A package and annually thereafter.

G-4.10 Privacy Impact Assessment (PIA) [G.5.6.4(10)]

The purpose of this task is to perform a PIA in compliance with GSA IT Security Procedural Guide 06-30 to assess the risk to individuals' privacy resulting from collecting, sharing, storing, transmitting, using, and/or disposing of personally-identifiable information (PII). To this end, we determine whether the BSS will store, process, and/or transmit PII and, if so, whether doing so presents any privacy risk to individuals. Based on the PIA outcome, we design controls into the system to protect PII, as necessary.

The first step in this task is to complete Part I of the PIA Template — PIA Contacts and Qualification Questions. These are functionally a Privacy Threshold Analysis (PTA) to determine if the BSS collects PII. Analysis consists of determining whether any of the following is true for the BSS:

- Collects, stores, or transmits PII in any identifiable form
- Collects, stores, or transmits PII from or about the public
- A PIA has been performed in the past
- There is or will there be a Privacy Act System of Records Notice (SORN).

We do not anticipate collecting, storing, or transmitting PII. However, if responses to the Qualification Questions indicate that BSS does or will collect, store, and/or transmit PII, then we complete the second step, which is to complete PIA Template Part II, System Assessment, and integrate the needed security controls in the BSS design and implementation. PIA Template Part II takes a structured approach leading to descriptions of the needed protection for system PII — specific data that must be protected; the SORN that the system operates under; assignment of accountability and responsibilities for protecting the PII; and the needed controls, including access/distribution restrictions.

We deliver a BSS PIA with the initial security A&A package and annually thereafter. Additionally, if PII is identified through the PIA Qualification Questions, we describe appropriate security controls in the SSP.

G-4.11 Configuration Management Plan [G.5.6.4(11)]

The purpose of this task is to develop and maintain a CMP in compliance with GSA IT Security Procedural Guide: *Configuration Management (CM)*, CIO-IT Security-01-05, and consistent with NIST SP 800-53, rev 4, guidance. The objective is to plan an orderly, documented, secure, and approved process for moving system changes through change management processes; updating configuration settings and baselines; maintaining system component inventories; controlling development, test, and operational environments; and developing, releasing, and updating key documents. To this end, we develop a BSS CMP that:

- Identifies roles, responsibilities, and configuration management processes and procedures.
- Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.
- Identifies the BSS configuration items and places them under configuration management.
- Identifies controls to protect the CMP from unauthorized disclosure and modification.

Unless directed otherwise by GSA, we base the BSS CMP on the Sample Outline for a Security Configuration Management Plan provided in NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, adapted as appropriate for the BSS.

We deliver a BSS CMP with the initial security A&A package and annually thereafter.

G-4.12 System(s) Baseline Configuration Standard Document [G.5.6.4(12)]

The purpose of this task is to develop and maintain a System Baseline Configuration Standard Document compliant with GSA CIO-IT Security 01-05 and consistent with NIST SP 800-53, rev 4, guidance. The objective is to establish and document baseline configurations that form the basis for future BSS system builds, releases, and/or changes. The steps in our process are to identify and document the following:

- A well-defined and current specification to which the BSS is built.
- The BSS baseline configurations, including BSS' components and communications and connectivity-related specifications.
- BSS architecture information such as:
 - Standard software packages installed on system devices
 - Operating system and application version numbers and patch information
 - Configuration settings/parameters
 - Network topology including the logical placement of BSS system components within the system architecture.

The initial baseline configurations reflect the architecture current at the time we develop the System Baseline Configuration Standard Document. We deliver the Document as part of the CMP with the initial A&A package. We revise the Document to reflect any BSS changes over time and deliver it annually.

G-4.13 System Configuration Settings [G.5.6.4(13)]

The purpose of this task is to develop and maintain system configuration settings, compliant with GSA CIO-IT Security 01-05 and NIST SP 800-53, rev 4, guidance. The objective is to configure the BSS' devices consistent with industry-recognized and validated security configuration settings. The steps that we take to identify and maintain the configuration settings are:

- Establish and document mandatory configuration settings for BSS IT products, reflecting the most restrictive mode without compromising operational requirements. Settings are in accordance with GSA technical guides, NIST standards, Center for Internet Security (CIS) guidelines (Level 1), and/or industry best practices.
- Configure the BSS in accordance with the identified mandatory configuration settings.
- Document the system configuration settings as part of the CMP and review and update as needed annually.
- Document and seek approval for any deviations from the approved baseline. We may find, for example, that a deviation from the mandatory configuration settings is required to enable one or more functional requirements. In such a case, we fully

document the situation, including any mitigating control(s) that reduce the risk of the deviation.

- Monitor and control changes to the configuration settings.

We deliver the system configuration settings as part of the CMP with the initial security A&A package and annually thereafter.

G-4.14 Incident Response Plan (IRP) [G.5.6.4(14)]

The purpose of this task is to develop and maintain an IRP that complies with IT Security Procedural Guide: *Incident Response (IR)*, CIO-IT Security-01-02, and is consistent with NIST SP 800-53, rev 4, guidance. The objective is to establish and communicate a coordinated incident response approach that includes coordinating and sharing incident information with external organizations, such as external service providers and organizations involved in the supply chain. Our approach is to do the following:

- Analyze and determine BSS-specific incident response requirements and characteristics, including:
 - A roadmap for implementing the incident response capability
 - The structure and organization of the incident response capability
 - A high-level approach for the BSS incident response that integrates with the environment in which the BSS operates
 - Definitions of reportable incidents and metrics for measuring the incident response capability
- Develop the IRP and distribute it to the individuals responsible for implementing the plan.
- Review the plan at least annually.
- Update the IRP to address any system/organizational changes or problems encountered during plan implementation, execution, or testing.
- Disseminate IRP changes, or the updated plan, to the individuals responsible for executing the plan.

We deliver the BSS IRP with the initial security A&A package and annually thereafter.

G-4.15 Incident Response Test Report (IRTR) [G.5.6.4(15)]

The purpose of this task is to test the IRP, document the results in an IRTR, and revise the IRP as needed in response to the testing. The objective is to verify that the IRP provides complete and current procedures for effectively responding to BSS-related security incidents. Test results show whether personnel responsible for the BSS were able to successfully respond to simulated incidents in accordance with the BSS IRP. We complete this task in compliance with GSA CIO-IT Security 01-02 and consistent with guidance in GSA IT Security Procedural Guide 06-29 and NIST Special Publications 800-53, rev 4; 800-61, rev 2, *Computer Security Incident Handling Guide*; and 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*. Although it is provided as a test report template for CP testing, we use the template provided in GSA IT Security Procedural Guide 06-29 for planning, executing, and reporting on our IRP testing.

That template provides a well-thought-out framework for Plan testing and reporting purposes, including a structure for identifying the test purpose and scope; incident response components to be tested; test objectives and other plans such as participants, required resources, logistics, and location(s); and test scenarios to be tested. Our test scenarios are the core of the plan, reflecting likely threats throughout the cyber-sphere in general as well as specific to the BSS environment and historical as well as potential incidents. We document each scenario on a Test Worksheet, providing expected results for each test. As we execute each IRP test, we document our findings and observations on the Test Worksheet; after analyzing the test findings, we document lessons learned and corrective action recommendations, if needed, and include those in the Test Worksheets. We then revise the IRP as necessary to improve the overall incident response process.

We deliver a BSS IRTR with the initial security A&A package and annually thereafter.

G-4.16 Continuous Monitoring of Security Controls of AT&T's System with a Continuous Monitoring Plan [G.5.6.4(16)]

The purpose of this task is to develop and maintain a Continuous Monitoring Plan to document how we accomplish BSS continuous monitoring consistent with guidance in

NIST Special Publications 800-43, rev 4, and 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*.

The objective is to provide the AO and BSS management with ongoing awareness of threats, vulnerabilities, and information security to support risk management decisions. With access to security-related information on a continuing basis, the AO and AT&T have the information necessary to make more effective and timely risk management decisions, including ongoing security authorization decisions. Our BSS Continuous Monitoring Plan consists of the following:

- The metrics to be monitored and evaluated in order to manage information security risk, such as vulnerability scan-related metrics including frequency; number of low-, moderate-, and high-risk vulnerabilities; and mean time to resolve findings.
- The frequency at which each metric is monitored.
- Planning for the ongoing security control assessments consistent with GSA's overall continuous monitoring strategy, such as for which controls are to be assessed in each year of a 3-year cycle.
- Procedures for correlating and analyzing security-related information generated by the monitoring and assessments.
- The actions to be taken in response to continuous monitoring outputs.
- The type(s), form, content, frequency, and distribution of security status reports.

Our implementing process includes:

- Assessing the information security implications of changes to the BSS and its operating environment through the configuration/change management process.
- Testing a subset BSS security controls, selected in accordance with GSA's overall monitoring strategy.
- Requiring proof that a selected subset of inherited controls is tested through those systems' ongoing security control assessments.
- Taking ongoing remediation actions based on the results of the ongoing monitoring activities, risk assessment, and outstanding items in the POA&M.
- Updating the SSP, SAR, and POA&M based on the results of the continuous monitoring process.

- Reporting the BSS' security status to the AO and others responsible for monitoring the system's security in accordance with the monitoring strategy.

We deliver the BSS Continuous Monitoring Plan with the initial security A&A package and submit continuous monitoring deliverables as required for each type, such as the POA&M submitted quarterly and the updated SSP submitted (at least) annually.

G-4.17 Plan of Action and Milestones [G.5.6.4(17)]

The purpose of this task is to develop and maintain a BSS POA&M as directed by the GSA IT Security Procedural Guide 06-30 and to manage vulnerability scanning findings through, and reported with, the quarterly POA&M submission consistent with GSA CIO-IT Security Guides 06-30 and 09-44, *Plan of Action and Milestones*, guidance and reporting instructions.

To this end, we develop and maintain a POA&M to document planned remedial actions to correct weaknesses or deficiencies from security assessments and continuous monitoring activities, including vulnerability scans. This enables us to implement a compliant, orderly, and approved process that yields risk and vulnerability status on an ongoing basis. All scans associated with the POA&M will be performed as an authenticated user with elevated privileges.

The POA&M captures the following elements, as required by the POA&M template provided in GSA CIO-IT Security Guide 06-30:

- Weaknesses/vulnerabilities
- Point of contact for remediation
- Additional resources needed to support remediation efforts
- Scheduled completion date and milestones with completion dates
- Milestone changes
- Source that identified the weakness/vulnerability
- Status.

We maintain the POA&M and update quarterly, including the required vulnerability scan and scan results. Scans will include all networking components that fall within the security accreditation boundary. We also annotate the POA&M based on annual system security User Certification/Authorization Reviews. We submit the POA&M as part of the A&A package, along with vulnerability scan outputs, and subsequently quarterly.

G-4.18 Independent Penetration Test Report [G.5.6.4(18)]

We understand that GSA or its independent contractor(s) perform internal and external penetration tests and prepare an Independent Penetration Test Report that they include with the security assessment package and annually thereafter. As discussed in the Security/Risk Assessment and Penetration Tests section below, AT&T supports GSA or their independent contractor(s) by providing needed coordination and facilitating physical and logical access to system devices within the Government Platform.

G-4.19 Code Analysis Reviews with Code Review Report [G.5.6.4(19)]

The purpose of this task is to conduct code analysis reviews in accordance with GSA CIO Security Procedural Guide 12-66, using the appropriate automated tools such as Fortify and Veracode. Through those reviews, we examine BSS code for common flaws, document results in a Code Review Report, and submit the report before we place the BSS into production, when there are changes to BSS code, and on an annual basis. The objective is to evaluate the effectiveness of security controls present in the BSS' source code and to determine the degree to which it may be vulnerable to attack due to insecure coding practices. Based on the review we can identify specific remedial steps that might be necessary to minimize risk. The ultimate goal is to reduce or eliminate potential software flaws.

Our methodology follows the

which,
at a high level, consists of
the following activities (see

Figure G-4.19-1):

We scale code analysis
activities to align with the
scope of the system being

reviewed. For BSS, much of the information gathering will have been accomplished through the SSP, with the addition of confirming the code analysis review objectives and requirements to establish and maintain the focus of the review. We also create a review plan to document the objectives and planned activities, tool(s), processes, participants, timing, and types of artifacts to be produced during the review.



Figure G-4.19-1. Secure Code Review.

We deploy a GSA-approved automated tool such as Fortify or Veracode, followed by a manual step to analyze and verify the scan output and, if necessary, additional static analysis to meet the review objectives. Finally, based on the review results, we prepare the Code Review Report, describing the application reviewed, the scope and objectives of the review, findings, and, if necessary, flaw remediation recommendations.

When applicable, we deliver the Code Review Report prior to placing BSS in production, annually thereafter, and whenever there are code changes.

G-4.20 Security/Risk Assessment and Penetration Tests [G.5.6.4(20)]

We understand that either GSA employees or GSA-designated third-party contractors perform the security/risk assessment and penetration tests, including control reviews, in accordance with NIST SP 800-53, rev 4, and NIST SP 800-53A, rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, and GSA IT Security Procedural Guide 06-30. Further, we understand that the assessments and tests include operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of government information, including the general support system infrastructure.

AT&T supports GSA as required by coordinating and facilitating needed access to enable GSA employees or GSA's independent contractors to conduct those A&A activities — control reviews including operating system, web application, and database vulnerability scanning of BSS components that process, store, and/or transmit government information.

G-4.21 Security/Risk Assessment Report (SAR) [G.5.6.4(21)]

As part of the A&A process, the independent assessor tests the BSS security technical, operational, and management controls and prepares a SAR to document any findings identified through that assessment. We develop corrective actions for those findings and translate each corrective action recommendation into a POA&M item. For each corrective action, we identify resources assigned to resolve the finding, planned actions, and due dates to track the status of planned remedial actions, as described in RFP Section G-4.17, Plan of Action and Milestones.

We maintain the POA&M throughout the system life cycle to document the responsibility for remedial actions to correct deficiencies identified in the SAR and to track and manage the status of planned remedial actions. Additionally, we document in the POA&M, remedial actions to close the gaps identified from our continuous monitoring activities, including vulnerability scans and annual security control assessments. Using GSA IT Security Procedural Guide 09-44 guidance and the *FY16 Plan of Action and Milestones (POA&M)* template, we deliver the original POA&M with the initial A&A package and quarterly thereafter.

G-4.22 Mitigation of Security Risks [G.5.6.4(22)]

We mitigate the security risks identified and confirmed through the security A&A and continuous monitoring activities. We understand that the Government determines the risk rating of BSS security vulnerabilities as critical/high-risk or moderate. We reflect the Government's risk rating in the scheduling of risk mitigation activities in the POA&M, with critical/high-risk vulnerabilities scheduled within 30 days and moderate-risk vulnerabilities within 90 days from the date they are identified. We make best-effort to resolve vulnerabilities within the required timeframe. We provide the Government with monthly status updates on any critical/high-risk vulnerabilities that have not been closed within 30 days, reflecting actions taken to date; factors contributing to the delay, such as a vendor's software changes; and projected resolution date.

G-4.23 Annual FISMA Assessment [G.5.6.4(23)]

The purpose of this task is to report the results of the annual FISMA assessment as required by GSA CIO IT Security Procedural Guide 04-26, *FISMA Implementation*, and guidance in NIST SP 800-53, rev 4.

The objective is to satisfy regulatory and policy requirements for initial and ongoing security authorizations, FISMA annual assessments, continuous monitoring, and system development life cycle activities. Doing so demonstrates that information security is built into the BSS, identifies any weaknesses and deficiencies throughout the life cycle, provides the AO with the information needed to make risk-based decisions as part of security authorization process, and demonstrates compliance with vulnerability mitigation procedures.

Our process begins with developing a FISMA security assessment plan as described in NIST 800-53, rev 4, control CA-2, Security Assessments, describing:

- The assessment scope, consisting of the BSS and its operating environment.
- The security controls and control enhancements that we assess. This is a subset of all required controls, determined in cooperation with GSA based on factors such as BSS' Moderate impact security categorization, the controls assessed in prior years' FISMA assessments, and risk, including status of the BSS POA&M.
- The assessment approach, methodology, and procedures that we follow to determine security control effectiveness. The procedures include analysis and re-use of existing current assessment results such as continuous monitoring outputs/vulnerability scan results.
- The assessment environment, team, and the team members' roles and responsibilities.
- Known constraints, assumptions and dependencies that may affect the assessment.
- Required resources for performing the assessment.
- Formalized assessment schedule.

We prepare for and execute a FISMA security assessment plan each year. Therefore, each year's plan addresses a different set of controls and control enhancements to be tested.

As we execute the FISMA security assessment plan, we record the implementation status (Implemented, Planned, or Pre-Planning) and test status (Not Tested, Not Satisfied, Partially Satisfied, or Fully Satisfied) for each control assessed along with how the BSS complies with each control in sufficient detail to provide the AO with assurance of the status. We deliver the results of the annual FISMA assessment results as directed by the GSA.

G-4.24 Policy and Procedure Documents [G.5.6.4(24)]

We develop policy and implementing procedures that address purpose, scope, roles and responsibilities, and compliance consistent with the applicable regulations and guidance for the policies identified in **Table G-4.24-1** NIST SP Policies.

Table G-4.24-1. NIST SP Policies. GSA and agency information in the AT&T BSS is secured through the implementation of the appropriate NIST SP Policies.

NIST SP Policy Name	RFP Reference
Access Control Policy and Procedures (NIST SP 800-53 R4: AC-1).	G.5.6.4(24)(a)
Security Awareness and Training Policy and Procedures (NIST SP 800-53 R4: AT-1)	G.5.6.4(24)(b)
Audit and Accountability Policy and Procedures (NIST SP 800-53 R4: AU-1) [G.5.6.4(24)(c)]	G.5.6.4(24)(c)
Security Assessment and Authorization Policies and Procedures (NIST SP 800-53 R4: CA-1)	G.5.6.4(24)(d)
Configuration and Management Policy and Procedures (NIST SP 800-53 R4: CM-1)	G.5.6.4(24)(e)
Contingency Planning Policy and Procedures (NIST SP 800-53 R4: CP-1)	G.5.6.4(24)(f)
Identification and Authentication Policy and Procedures (NIST SP 800-53 R4: IA-1)	G.5.6.4(24)(g)
Incident Response Policy and Procedures (NIST SP 800-53 R4: IR-1)	G.5.6.4(24)(h)
System Maintenance Policy and Procedures (NIST SP 800-53 R4: MA-1)	G.5.6.4(24)(i)
Media Protection Policy and Procedures (NIST SP 800-53 R4: MP-1)	G.5.6.4(24)(j)
Physical and Environmental Policy and Procedures (NIST SP 800-53 R4: PE-1)	G.5.6.4(24)(k)
Security Planning Policy and Procedures (NIST SP 800-53 R4: PL-1)	G.5.6.4(24)(l)
Personnel Security Policy and Procedures (NIST SP 800-53 R4: PS-1)	G.5.6.4(24)(m)
Risk Assessment Policy and Procedures (NISTSP 800-53 R4: RA-1)	G.5.6.4(24)(n)
Systems and Services Acquisition Policy and Procedures (NIST SP 800-53 R4: SA-1)	G.5.6.4(24)(o)
System and Communication Protection Policy and Procedures (NIST SP 800-53 R4: SC-1)	G.5.6.4(24)(p)
System and Information Integrity Policy and Procedures (NIST SP 800-53 R4: SI-1)	G.5.6.4(24)(q)

We review and verify the policies in **Table G-4.24-1** as part of the initial security assessments and update as needed. We submit updates to the GSA COR/ISSO/ISSM as they occur or at least biennially. The system owner and/or designated ISSO review the policy. In turn, all required changes are communicated to the AT&T ISSO for incorporation into the policy and procedures document. Once accepted by all parties, we disseminate the documents to organizational entities and individuals responsible for implementing the policies and procedures. We also review and update the security awareness and training policy and procedures as necessary but at least annually. These policies are consistent with the applicable NIST Special Publications and GSA IT Security Procedural Guides.

G-5 Additional Security Requirements [G.5.6.6; Section I]

We comply with the following requirements, as we have done on the Networx contract, and other federal contracts:

- Adhere to proper privacy and security safeguards in accordance with the FAR Part 52.239-1. (See Section I.)
- Label the deliverables identified in Section C.6.6 “CONTROLLED UNCLASSIFIED INFORMATION” (CUI) or AT&T selected designation per document sensitivity.

- Encrypt external transmission/dissemination of CUI data to or from a GSA computer. Use certified encryption modules in accordance with FIPS PUB 140-2 & 140-3, “Security Requirements for Cryptographic Modules.”
- Where appropriate, ensure implementation of the requirements identified in the FAR (see Section I, 52.224-1, “Privacy Act Notification” and FAR 52.224-2, “Privacy Act.”)
- Cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the federal government’s agent. In this connection, note that **Appendix B** describes in greater detail our approach to protecting the government’s information systems, and information with our supply chain controls.
- Understand/acknowledge that the government has the right to perform manual or automated audits, scans, reviews, or other inspections of the AT&T’s IT environment being used to provide or facilitate services for the government.

In accordance with the FAR (see Section I, 52.239-1) we are responsible for the following privacy and security safeguards:

1. We do not publish or disclose in any manner, without the CO’s written consent, the details of any safeguards either designed or developed by AT&T under this contract or otherwise provided by the government (except for disclosure to a consumer agency for purposes of security A&A verification).
2. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public government data collected and stored by us, we provide the government logical and physical access to our facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits include, but are not limited to, 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
3. Automated scans can be performed by government personnel, or agents acting on behalf of the government, using government operated equipment, and government specified tools.

If we choose to run our own automated scans or audits, results from these scans may, at the government's discretion, be accepted in lieu of government performed vulnerability scans (See GSA Security Guide 6-30 "Managing Enterprise Risk" for acceptance criteria).

In these cases, scanning tools and their configurations are approved by the government. In addition, we provide, in full, the results of our scans to the government.

G-5.1 Personnel Security Suitability [G.5.6.6.1; Section I]

We have a detailed and mature process for administering the application for HSPD-12 background investigation. We grant access to government information, within the security A&A scope, only to personnel who attain this credential by successfully submitting a timely application for background investigation and are granted suitability by the GSA, in accordance with FAR Part 52-204-9 with Section I, Homeland Security Presidential Directive-12 (HSPD-12), OMB guidance M-05-24, M-11-11 and as specified in GSA CIO Order 2100.1I and GSA Directive 9732.1D Suitability and Personnel Security. We understand that the government is responsible for the cost of such background investigations.

Table G-5.1-1 shows the security-related deliverables that are required for the BSS. We deliver them, as discussed in the corresponding sections of our proposal.

Table G-5.1-1. BSS Deliverables. *AT&T Provides Required Deliverables as Described in the Cited Sections.*

Deliverable	Proposal Section
Interconnection Security Agreements with the initial security A&A package to include annual updates	G-4.2
Control Tailoring Workbook with the initial security A&A package	G-4.3
GSA NIST SP 800-53 R4 Control Summary Table with the initial security A&A package	G-4.4
RoB with the initial security A&A package to include annual updates	G-4.5
System Inventory with the initial security A&A package to include annual updates	G-4.6
CP, DRP, and BIA with the initial security A&A package to include annual updates	G-4.7
CPTP with the initial security A&A package to include annual updates	G-4.8
CPTR with the initial security A&A package and annually thereafter	G-4.9
PIA with the initial security A&A package to include annual updates	G-4.10
CMP with the initial security A&A package to include annual updates	G-4.11
System Baseline Configuration as a part of the CMP, submitted with the initial security A&A package to include annual updates	G-4.12
System configuration settings, included as part of the CMP and updated and/or reviewed annually	G-4.13
IRP with the initial security A&A package to include annual updates	G-4.14
IRTR with the initial security A&A package to include annual updates	G-4.15
Continuous Monitoring Plan with the initial security A&A package to include annual updates	G-4.16

Deliverable	Proposal Section
POA&M as part of the initial security A&A package followed by quarterly updates	G-4.17
Appropriate vulnerability scan results submitted with the initial security A&A package	G-4.17
Annual information system User Certification/Authorization Review annotated on the POA&M	G-4.17
If applicable, a Code Review Report submitted as an initial deliverable prior to placing the information system into production, when there are code changes, and annually	G-4.19
Security/Risk Assessment and Penetration Tests	G-4.20
Track Security/Risk Assessment Report Findings in a POA&M	G-4.21
Mitigate Security Risks Found During the A&A and Continuous Monitoring	G-4.22
Deliver Annual FISMA Assessment Results Each Fiscal Year	G-4.23
Develop and Maintain Policies and Procedures as Outlined in the NIST SP 800-53, rev 4, and Appropriate GSA IT Security Procedural Guides	G-4.24



General Services Administration (GSA)

Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

Appendix H — NS/EP Functional Requirements Implementation Plan

APPENDIX H — NS/EP FUNCTIONAL REQUIREMENTS IMPLEMENTATION PLAN [L.30; L.30.2.8; M.2.2 (7 OF 7); G.11]

Since the establishment of the Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) Emergency Communications Division (ECD), formerly the National Communications Systems (NCS) in 1963, AT&T has worked closely with the ECD to develop National Security and Emergency Preparedness (NS/EP) telecommunications infrastructure capabilities for circuit-switched and packet-enabled networks. AT&T developed and has been supporting the Government Emergency Telecommunications Service (GETS) and NS/EP functionality and systems since they were envisioned over 30 years ago. We are directly involved in major transitions of the NS/EP Telecommunications Infrastructure to Internet Protocol (IP) and digital packet switched networks from legacy circuit-switched systems.

This **Appendix H** constitutes our NS/EP Functional Requirements Implementation Plan and addresses the requirements of RFP Sections G.11.1-G.11.3. This plan will be updated annually and provided to the government in compliance with deliverable #83 in RFP Table F.2.1.

AT&T is committed to continually providing and improving robust NS/EP services and functionality. We are committed to providing prompt, robust and effective support under conditions of stress that might affect the telecommunications infrastructure ranging from crises or natural disasters through declared conditions of NS/EP. For example:

- Under the Networkx contracts with GSA, AT&T currently supports all required basic NS/EP functional requirements across the communications services we provide.
- AT&T maintains a robust disaster response infrastructure, including organized teams, equipment, and processes that have deployed successfully in multiple crises.
-
- The ECD and AT&T have influenced the telecommunications industry to develop standards that provide end-to-end priority and Quality of Service (QoS) across all services and carriers. These standards provide the ability to implement prioritized advanced capabilities within the AT&T networks.
- AT&T advocates to various standard organizations such as, Alliance for Telecommunications Industry Solutions (ATIS) and International Telecommunication

Union (ITU), for the ability to provide priority treatment of NS/EP services over IP infrastructures.

- Based upon specific Task Order (TO) assignments from the ECD to encompass improvements in technology and our own testing and research, AT&T design engineers, operations, and support staff monitor and enhance Priority Telecommunications Services (PTS) for the ECD in a continual improvement process.
- AT&T and the ECD are developing next generation NS/EP features that will provide priority across a wide variety of services and applications.

Table H-1 describes the benefits of the AT&T NS/EP approach and capabilities.

Table H-1. AT&T NS/EP Approach and Capabilities. *Networks and services provided under EIS derive substantially enhanced reliability, responsiveness and technological innovation from AT&T leadership in the development and implementation of NS/EP functionality.*

Evaluation Factor	Approach	Benefit	Capability
Quality of Systems	▪ The AT&T backbone network capitalizes on its immense size and employs self-healing technology	▪ GSA users receive continuous, high quality service as the network is able to respond to huge increases in traffic or degradation even before NS/EP services are invoked	▪ AT&T has the nation's most reliable 4G Long-Term Evolution (LTE) network ▪ The AT&T overall voice and data network now covers more than 99 percent of all Americans ▪ The AT&T mobile Internet service covers more than 90 percent of the U.S. population, including all major U.S. markets ▪ The AT&T support to Network customers provides the 14 NS/EP Functional Requirements for all 17 Network services
Customer Access	▪ AT&T fully integrates NS/EP functionality with its commercial infrastructure ▪ AT&T maintains disaster response equipment and staff	▪ Customers have access to one of the world's largest networks with fully modernized technology ▪ Customers receive rapid restoration of service	
Ability	▪ AT&T actively participates in discussions with the ECD to advise and advocate with peers on future needs	▪ Ease of transition ▪ Established processes and technologies	

Under the EIS contract, AT&T continues our partnership with GSA and the ECD in the development and implementation of NS/EP functional capabilities across the full range

of EIS services and other service elements throughout the life of the contract. AT&T considers Executive Orders (EO) 12472 and 13618 and its successors in the design and operations of services provided under this contract, and provides EIS services and other service elements (technical, management and operations-related) that are fully compliant with national policy and national policy directives including:

- PL 93-288 (Disaster Preparedness Assistance, dated May 22, 1974)
- PPD-1 (Organization of the National Security Council System, dated February 13, 2009)
- PPD-21 (Critical Infrastructure Security and Resilience, dated February 12, 2013)
- NSDD-97, NSDD-145 and its successors
- Other applicable laws, regulations, and directives

AT&T will notify the government in a timely manner (in a format similar to the “Abnormal Report” we currently furnish to the Department of Homeland Security [DHS] National Coordination Center) when events arise that may have major consequences on the AT&T network. In such cases, AT&T seeks the government’s priorities, but knows that we continue to have sole responsibility for the AT&T network. In addition, AT&T alerts the government and the ECD to network changes or newer technology, which may impact government functions or offer the potential for service improvements.

H-1 Basic Functional Requirements [G.11.1]

Our ongoing commitment to support a robust set of NS/EP functions and services gives agencies the ability to accomplish their critical missions under the most challenging natural and man-made circumstances. In the event of crisis or nonstandard events, our network has the capacity, resilience, and operational procedures to support NS/EP users. AT&T fully supports the 14 basic functional requirements for NS/EP telecommunications and Information Technology (IT) services covered in detail in the subsequent paragraphs. These requirements are identified by the DHS, ECD, and the Office of Science and Technology Policy (OSTP) for NS/EP telecommunications services, are now being endorsed by American National Standards Institute (ANSI) T1 and International Telecommunication Union (ITU)-TSS standard bodies and widely supported by telecommunications carrier communities.

AT&T fully understands the complexity of accomplishing the 14 NS/EP supported basic functional requirements and updates our support of them as ECD directs. AT&T is committed to providing and improving its NS/EP support for the lifespan of the EIS contract and beyond. AT&T is already working for ECD to address the retirement of older Time Division Multiplexing (TDM) technology and signaling methods by all major carriers, such as traditional coin operated phones and TDM-based core and access switch Frame Relay. All of the technology GSA uses must still be maintainable, but only within the offerings of the commercial carriers upon which NS/EP rides.

H-1.1 Enhanced Priority Treatment [G.11.1(1)]

Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic.

AT&T provides response to varying congestion levels in AT&T NS/EP for optimal communications throughput. AT&T gives NS/EP mission-related voice and data services preferential treatment over other traffic through a combination of:

1. GETS service (including Number Translation [NT] Service)
2. Telecommunications Service Priority (TSP) program (detailed in **Section H-3.3** below)
4. Wireless Priority Service (WPS) (covered in detail in **Section H-3.2** below)
5. Inherent characteristics of the various commercial service offerings such as priority service and QoS

H-1.2 Secure Networks [G.11.1(2)]

Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.

All access to NS/EP is strictly controlled, monitored and is fully certified to meet all National Institute of Standards and Technology (NIST) standards and DHS/ECD requirements. AT&T provides NS/EP users with access (including agency-approved classified access) to GETS and WPS as part of the daily routines within NS/EP. Our personnel already possess the government security clearances and operate daily under strict government and military agency security and information handling procedures.

H-1.3 Non-Traceability [G.11.1(3)]

Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).

Non-traceability is provided by the GETS NT service in NS/EP. With the enhanced security provided by AT&T NS/EP NT service, agencies use NS/EP voice priority services without risk of usage being traced. AT&T began offering NT service on May 23, 1986 and has continued to serve critical users ever since.

Our switches identify NT calls by using the portions of the dialed number. NT call attempts have a high-completion rate, even under conditions of severe congestion in the Public Switched Telephone Network (PSTN) because they receive GETS priority treatment in the AT&T network. **Table H-2** describes numbers translation features.

Table H-2. AT&T Number Translation Service. *GSA users receive benefits that go beyond non-traceability from AT&T feature rich Number Translation Service and advanced technology.*

Key Features of AT&T 4ESS Switch Based NT Service
▪ Numbering plan removes any geographic relevance in the dialed number ▪ Call is entirely processed without requiring access to external databases ▪ NS/EP NT is a robust service using GETS features and capabilities, and therefore provides an enhanced rate of call completion ▪ NS/EP NT calls have an improved probability of completion at times of network congestion due to Enhanced Real-Time Network Routing (E-RTNR), GETS End-to-end Class of Service (ECOS), and exemptions from restrictive Network Management Controls (NMCs) ▪ NT NS/EP capability is available 24x7 to certified users

As an example of continuous security improvements by AT&T, at the direction of the DHS in 2006, the NT service architecture was modified to provide designated users the ability to enter a Personal Identification Number (PIN) when placing NT calls. As part of our “forward-looking” architecture, this capability was developed in the AT&T Voice over Internet Protocol (VoIP) network. TDM-originated NT calls are routed from the Series 4 Electronic Switching System (4ESS) network to the AT&T VoIP network where the user is then prompted to enter their PIN. After successful PIN authentication, the Application Server internal database is accessed to translate the dialed NT number to the actual Numbering Plan Area (NPA)-NXX, and the call is routed through the AT&T VoIP and TDM networks to the appropriate destination. If there are any problems processing the NT call in the VoIP network, the 4ESS switch based NT features described above will still be available to process the call. This fail-safe mechanism also continues to provide priority treatment features during times of network congestion.

H-1.4 Restorability [G.11.1(4)]

Should a service disruption occur, voice and data services must be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.

In addition to the Edge switch fail-safe switch mechanisms described in RFP Section H-1.3, the AT&T network has resiliency and redundancy and is fully meshed.

Message recovery via MPLS routing is built in. Our network is restorable and recoverable via TSP guidelines including local provider “last mile” and repair and

replacement materials. In addition to interfacing with

local vendors at sites of disruptions, AT&T has its Network Disaster Response (NDR) teams to restore services (especially subsequent to natural disasters).

As a unique capability, AT&T maintains a ready fleet of five large NDR teams that will be called upon within hours to dispatch from secure facilities to restore communications services after natural or man-made

disasters, as depicted in **Figure H-1**. They can deploy up to 100 vehicles in a group to rapidly engage into a disaster area and operate standalone and unsupported up to 40 days. Once services are restored, the mobile

teams can have elements remain in place to provide services for up to two years. In 2011 a devastating tornado struck Joplin Missouri, our teams remained in place until critical infrastructure, and buildings were designed and constructed. One team

is designed as a flyaway group and

can be dispatched to Europe or Africa. NDR team members are highly trained volunteers and are regularly given training drills and practice deployments to enhance their readiness status. On average, these five teams are deployed for actual events 40-50 times a year.

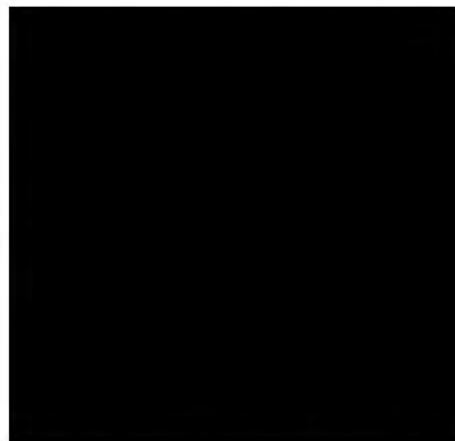


Figure H-1. National Disaster Recovery Team Equipment.
Our NDR teams will provide a wide range of emergency services on short notice.

In addition to the NDRs (which are focused on larger scale or higher-priority responses), AT&T provides locally developed, situation-specific, commercial response teams and capabilities. For instance, at local building complexes the NDR team can provide Points of Presence (PoP), backbone network nodes and Central Offices.

AT&T also provides FEMA responder and agency post-disaster communications capability that:

- Assess communications needs of the responder organizations and warehouses and offices expected to deploy near a disaster location
- Determine surviving communications
- Develop an interim solution and longer-term communications capability
- Coordinate service with Federal Emergency Management Agency (FEMA) for restoration and recovery using suitcase fly-in kits and Cells on Wheels (COW) as needed for FEMA to support Field Offices (FO), and multi-agency Joint Field Offices (JFO) administered by FEMA and these NS/EP users.

H-1.5 International Connectivity [G.11.1(5)]

Voice and data services must provide access to and egress from international carriers. AT&T is the largest international carrier and stands as a global network.

We have our own international communications available internally and we regularly interoperate with local and international carriers in 200 countries.

International connectivity is thus already available for the NS/EP mission. Full NS/EP priority cannot be assured over foreign carriers but will be available at

the end points and over all AT&T US network components. Our international telecommunications network is self-contained and is not exposed to internet hazards.

H-1.6 Interoperability [G.11.1(6)]

Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks, which will be identified after contract award.

As a large-scale telecommunications company, AT&T has a history of providing interoperability for its NS/EP services through its technical and business relationships

Did You Know?

AT&T delivers voice service in more than [REDACTED] and data service in more than 210 countries, including fast

[REDACTED] The AT&T network uses GSM technology, the global technology standard upon which the vast majority of the world's wireless services operate.

with the array of other carriers, tribal and government systems, and private networks. Interoperability is also positively impacted by our active participation and leadership on industry standards committees. Security is maintained even while transiting overseas carriers or end points. The one restriction is that NS/EP priority of service cannot be guaranteed when using overseas carriers other than AT&T. Full services are maintained along the United States network components of the message links.

H-1.7 Mobility [G.11.1(7)]

The ability of voice and data infrastructure to support transportable, re-deployable, or fully mobile voice and data communications.

AT&T NS/EP services already support full mobility capabilities for voice and our network is data capable. WPS will be further enhanced to operate in networks with newer technology such as the anticipated 5G communications in the future. AT&T offers GSA a large commercial-based mobile network with over \$160 billion invested in infrastructure for supporting mobile communications and nearly \$23 billion reinvested annually to expand and improve it. AT&T has flexibility to support large events such as DHS-designated National Special Security Events (NSSE), Presidential inaugurations, large concert venues, National Association for Stock Car Auto Racing (NASCAR) races, papal visits, major sports events, as well as disasters with mobile network resources such as Cells on Wheels (COW) and similar local nodes for temporary increases in capacity.

The NDR team possesses large-area coverage support for nearby first responders as well as meeting their own field deployment needs. They often assist local police, emergency medical services, fire departments and NGAs (Non-Governmental Agencies e.g., The American Red Cross) in search and rescue (SAR) and recovery. Using industry standard components allows GETS and NS/EP to be used in these circumstances. AT&T has significant commercial network contingency mobile units deployed as well.

H-1.8 Nationwide Coverage [G.11.1(8)]

Voice and data services must be readily available to support the national security leadership and inter- and intra- agency emergency operations, wherever they are located.

Between our considerable nationwide mobile and landline coverage and roaming use of other carriers' resources, EIS is provided full nationwide coverage. Our network coverage joined with that of compatible carriers is already considerable and expansive, with continued expansion to buildings, tunnels, and large venues such as concerts and sporting events including all major U.S. markets. The current NS/EP interoperable mobile and landline features combined with our own mobile network coverage was demonstrated as successful in the September 11, 2001 disaster, Hurricane Katrina, 9/11, super storm Sandy, and numerous local incidents and events.

H-1.9 Survivability/Endurability [G.11.1(9)]

Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.

AT&T backbone network resources were engineered specifically with nuclear war survivability considered, with robust engineering of services and infrastructure that enhances the survivability and durability in natural and manmade disasters. The sheer size of our worldwide network is a major factor in providing NS/EP survivability/durability. In addition, through mesh designs with redundancies and multiple interconnects and automated control features, rapid response is enhanced, and restoration of full services are expedited. The backbone network is described as self-healing since the internal controls will sense and react to any disruptions by rerouting traffic as required, alerting system managers to the actions taken, dispatching repair and restoration resources, and automatically reinstating system resources to the network as soon as recovery and restoration are completed. The tremendous bandwidth of the AT&T networks means a great deal of increased traffic or degradation must occur before any significant impact upon regular users, let alone NS/EP priority users, is noted.

H-1.10 Voice Band Service [G.11.1(10)]

The service must provide voice band service in support of presidential communications.



Figure H-2. White House Support.

AT&T has been providing White House voice band service since the 1950s.



H-1.11 Broadband Service [G.11.1(11)]

The service must provide broadband service in support of NS/EP missions.

AT&T services currently accept GETS calls from any broadband service via standard commercial business VoIP AT&T network interface.

H-1.12 Scalable Bandwidth [G.11.1(12)]

NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements.

AT&T NS/EP services as implemented on our network have full scalability resulting from use of our global network capacities and resiliency and is offered as a feature in Network on Demand. The AT&T network already has the capability to deal with daily, seasonal and incident-related traffic volume variations. It has enough meshed capability to be self-healing and reroute around any natural causes or man-made disruptions, alert system managers to the actions taken, and automatically resume service once the disruption has been eliminated. With NS/EP priority services, several levels of actions are available to deal with effectively scaling up the access of NS/EP users to more network resources when mission needs change or when infrastructure has been

seriously damaged. Available AT&T bandwidth far exceeds full demand of all NS/EP users.

H-1.13 Affordability [G.11.1(13)]

The NS/EP service must use network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services).

NS/EP employs commercial carriers such as AT&T to accomplish its mission and services as needed, enjoy economies of scale, and lower costs through use of COTS elements of the network and interoperability with industry standard devices. All of our NS/EP services have been designed and implemented leveraging the breadth and strength of the AT&T commercial network. AT&T exemplifies the value of the government approach by providing NS/EP functionality as add-ons to its infrastructure and service offerings. As AT&T invests in its future, we are making modifications to NS/EP ECD functionality to take advantage of technology advances, improved security, lower costs, and improved features of LTE and more using IP-based systems.

H-1.14 Reliability/Availability [G.11.1(14)]

Services must perform consistently and precisely according to their design requirements and specifications and must be usable with high confidence.

In situations ranging from simple interagency priority communications to responding to major national/international incidents, AT&T NS/EP enabled services have been able to provide the highest levels of reliability and availability through:

- Engineering design
- Robust and high-availability network (more than 99.999% reliability)
- Self-healing features
- Secure and trusted suppliers, enforcing compliance, and requiring our teammates and subcontractors to do the same

Our superior capabilities have been demonstrated in past national and local incidents. Even with the severe congestion experienced by people in New York and Washington DC on 9/11/2001, 96% of AT&T GETS calls connected in less than 90 seconds and were completed on the first attempt.

H-2 Protection of Classified and Sensitive Information [G.11.2]

AT&T recognizes that NS/EP-related information includes but is not limited to databases for classified information; critical users' locations, identifications, authorization codes, and call records; and customer profiles. In addition, AT&T is provided access to certain classified and sensitive materials required for the planning, management, and operations for NS/EP. That information is in various forms, including hardcopy and electronic media. AT&T identifies all sensitive and classified material and information as to its classification and protects it in accordance with applicable industrial security regulations (National Industrial Security Program Operating Manual [NISPOM] and National Security Agency (NSA)-approved standards as applicable for safeguarding classified information). The level of classification is up to and including TS/SCI (Top Secret/Sensitive Compartmented Information), and identified by the government. AT&T protects and stores all classified materials within government-approved facilities appropriate for the level of classification and has in-house SCIFs (Sensitive and Classified Information Facilities) only to be used under strict government-approved secure handling, cataloging, retention and destruction guidelines. Besides facilities, our personnel already possess the government security clearances and operate daily under strict government and military agency security and handling procedures. Documents and data used in vetting and providing NS/EP users' access to GETS, TSP and WPS are protected as part of the daily routines within NS/EP.

H-3 Department of Homeland Security Emergency Communications Division Priority Telecommunications Services [G.11.3]

AT&T is fully committed to complying with and interoperating with all DHS ECD PTS, which requires integrated components including:

- TDM GETS service (including Number Translation)
- TSP program
- WPS
- Next Generation Internet Protocol (IP) GETS capabilities (including Number Translation)
- Inherent characteristics of the various commercial service offerings

AT&T cooperates fully with the ECD's Communications Portfolio Management (CPM) branch to coordinate our actions and to provide the NS/EP communications community access to priority telecommunications and restoration services to communicate under all circumstances.

AT&T is committed to continually providing robust NS/EP services and works closely with ECD to develop next generation GETS over IP. ECD and AT&T are influencing the telecommunications industry to develop standards that provide end-to-end priority and QoS across all IP services. These standards provide the ability to implement prioritized advanced data capabilities within the AT&T IP MPLS TE networks. AT&T continues to advocate to various standard organizations for the ability to provide priority treatment of NS/EP services over IP infrastructures.

H-3.1 Government Emergency Telecommunications Service [G.11.3.1]

GETS is valuable whenever there is a critical need to communicate, especially during natural or man-made disasters, or when there is a situation resulting in network congestion and/or damage.

The AT&T network consists of both the legacy TD network and the IP network that supports Voice over Internet Protocol (VoIP), as shown in **Figure H-3.1-1**

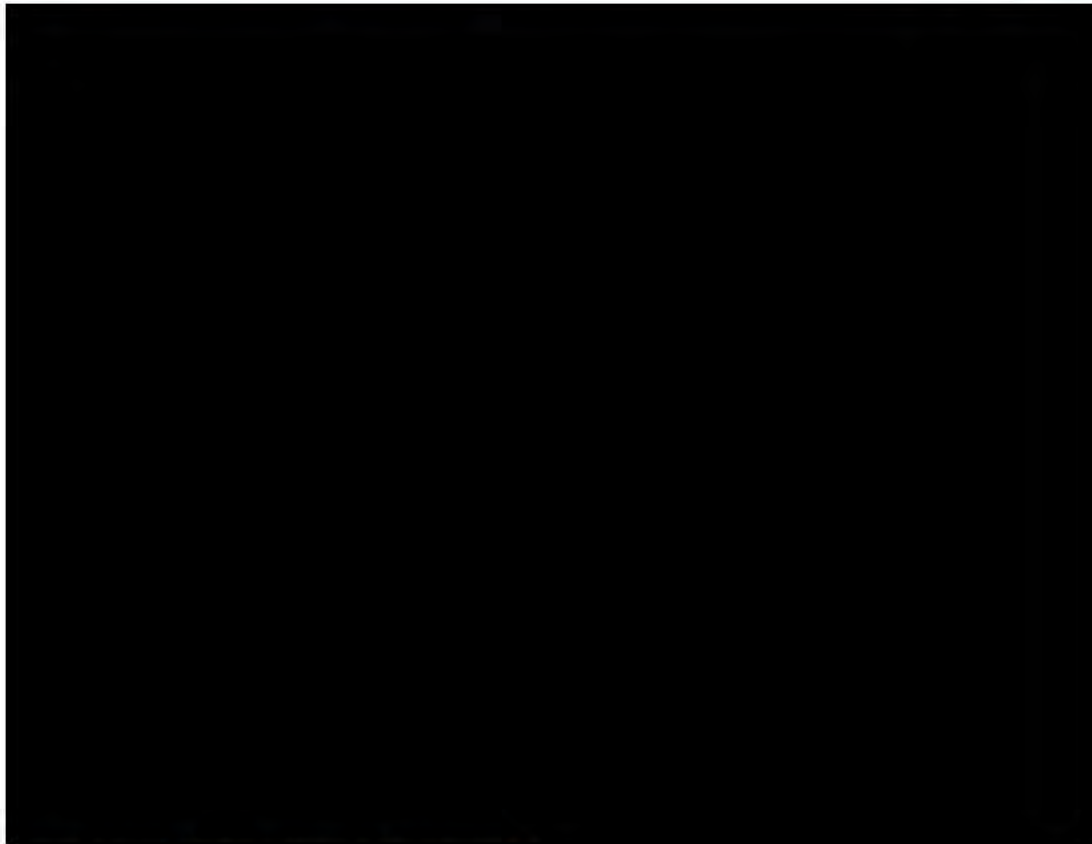


Figure H-3.1-1: AT&T's Network Architecture.



Figure H-3.1-2 shows the process and prioritization applied to a GETS enabled TDM call.

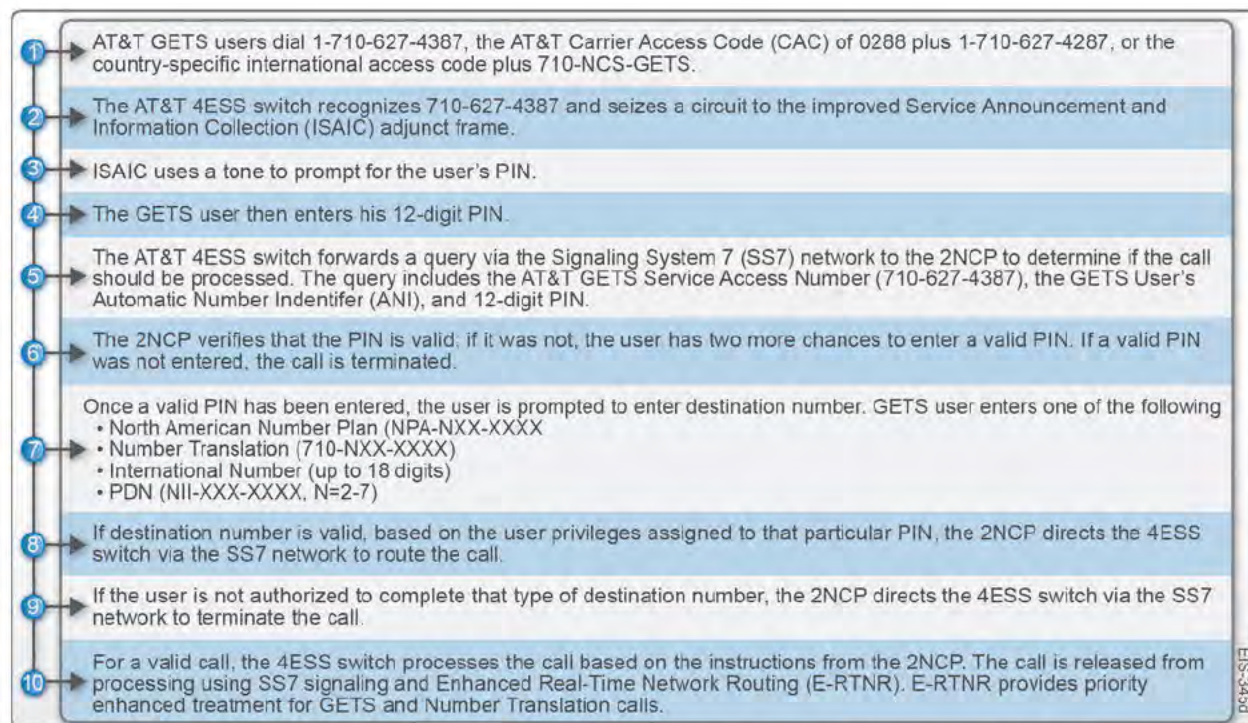


Figure H-3.1-2. GETS Enabled TDM Call Processing. GSA's GETS users are able to follow a simple process with high-reliability based on AT&T advanced GETS enabled architecture.

GETS is available 24x7 to government-designated users. Users are authenticated by entering a valid 12-digit PIN to gain access to GETS. The user is then able to enter a destination number. If a GETS user has the appropriate privileges for the destination dialed (i.e., domestic, international, Pseudo Destination Number [PDN], NT) the call is allowed to proceed.

Figure H-3.1-3 shows the AT&T TDM architecture that already provides GSA compatibility with NS/EP services. The architecture has been tested and recognized as highly effective on Networkx and other contracts. Priority treatment is provided at the 4ESS switches for GETS calls by using the ECOS feature and the Repetitive Routing Attempt Procedure (RRAP), while trunk queuing is provided on the 5ESS and DMS-250 edge switches.



Figure H-3.1-3. AT&T GETS TDM Architecture Modifications.

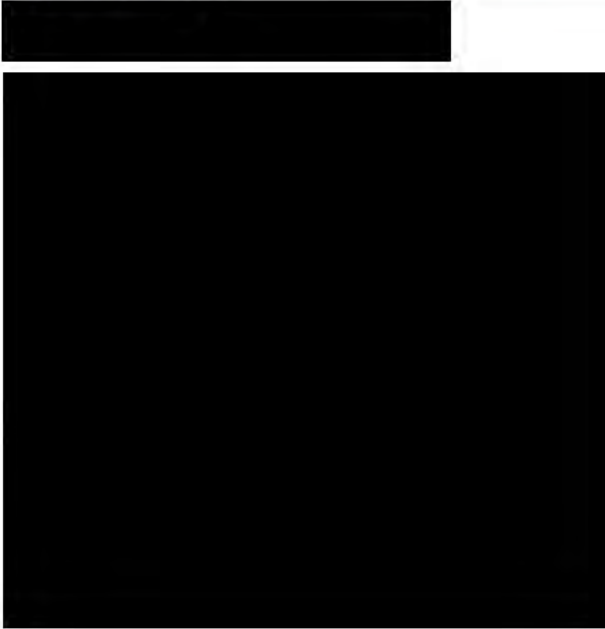


GETS calls are identified by the High Probability of Completion (HPC) capability involving the use of a special coding for the calling party category (CPC) parameter in the initial address message (IAM) associated with a GETS call to identify a NS/EP call that requires priority treatment. The priority of the IAM within the AT&T Switched Network (ASN) is controlled by the message transfer part (MTP) priority level parameter.

The SS7 Initial Address Message (IAM) Message Transfer Part (MTP) priority level is set one higher than the value assigned to Plain Old Telephone Service (POTS) traffic in the AT&T network.

E-RTNR provides additional routing features within the 4ESS network for GETS calls. Both the 4ESS switches and edge switches are capable of recognizing GETS calls (based on the access number 710-NCS-GETS) and setting the Calling Party's Category (CPC) parameter to NS/EP in Signaling System 7 (SS7) signaling messages. GETS includes a customer-controlled fail-open feature in the 4ESS switches to mitigate unlikely situations where a GETS call cannot access the No. 2 Network Control Point (2NCP) for PIN validation. The government has directed AT&T to have the fail-open parameter set to "on," so that such a call is routed through the network. The NS/EP Control Center (CC) in Bedminster, New Jersey validates all fail-open GETS calls. AT&T enables worldwide access to the AT&T Switched Network (ASN) through a universal access number, 710-627-4387 (710-NCS-GETS), with priority call routing and treatment.

Figure H-3.1-4



1	An NS/EP call originating behind an AT&T TDM switch reaches the NGBE via SS7 signaling.
2	The NGBE recognizes the call as NS/EP based on the access number (710-NCS-GETS) or Calling Party's Category (CPC)=NS/EP setting. The NGBE formulates a Session Initiation Protocol (SIP) INVITE to be sent to the NS/EP AS. The NGBE will insert a Resource Priority header (RPH) in the INVITE message with RPH set to ets.0.
3	The NS/EP AS receives the INVITE from the NGBE. The NS/EP AS recognizes the call as NS/EP based on the Dialed Number (710-NCS-GETS) or RPH=ets.x.
4	The AS signals the Media Server (MS) to be engaged on the call to collect PIN and Destination Number.
5	The MS receives the SIP INVITE, retrieves the Voice Extensible Markup Language (VXML) script from the AS, and establishes a media path to the originating NGBE to collect user inputs.
6	After hearing the tone, the user enters a PIN. The user is given three chances to enter a valid PIN; if after three tries, no valid PIN was entered, the NS/EP AS terminates the call. If a valid PIN was entered, the user is prompted to enter a Destination Number. The MS sends these results to the NS/EP AS using Hypertext Text Transport Protocol (HTTP).
7	NS/EP AS verifies that the user has the appropriate privilege to call the Destination Number. If the user does not have the necessary privilege, the NS/EP AS terminates the call; otherwise, the AS instructs the MS to play the AT&T branding announcement.
8	The AS sends a SIP BYE the MS, and the MS is dropped from the call.
9	The AS then sends a SIP INVITE to the RS.
10	A Local Number Portability (LNP) dip will be performed if necessary. The RS will return a maximum of 4 route-lists to the AS.
11	The AS will pick the egress NGBE for routing the call based on the route list received from the RS.
12	AS sends a SIP INVITE to the terminating NGBE, along with information on setting up a Real-Time Protocol (RTP) session with the originating NGBE.
13	Terminating NGBE interacts with the terminating LEC network.
14	Terminating NGBE sends a SIP 180 RINGING back to the AS.
15	The AS sends a SIP message to the originating NGBE with information that will allow a media path to be set up between the originating and terminating NGBEs.
16	Media path is established between originating and terminating NGBEs.

Figure H-3.1-4: GETS enabled IP Call Processing. Agency workers are fully supported by the AT&T IP network when sending GETS calls

Session Initiation Protocol (SIP) messages are used to set-up and tear-down calls within AT&T's IP network. Calls are given SIP transport priority and SIP processing priority. SIP transport priorities are determined by network elements setting the appropriate Differentiated Services Code Point (DSCP) (also known as DiffServ Code Point) in IP packets. This ensures that NS/EP signaling messages are transported with appropriate priority. The SIP processing priority is determined by the network elements setting Resource Priority Header (RPH) in the SIP message; this ensures that resources are allocated to process signaling messages.

Media transport priority is provided by assigning packets of traffic CoS designations using appropriate DSCP. During periods of congestion, these CoS designations

exempt IP NS/EP calls from call admission controls, network management controls, and machine congestion controls. They also make necessary bandwidth available and provide these packets with the necessary priority when queued.

H-3.2 Wireless Priority Service [G.11.3.2]

AT&T Mobility offers wireless services with GETS capabilities fully compliant and interoperable with ECD's WPS. AT&T WPS provides a comprehensive set of capabilities meeting all 14 NS/EP functional requirements that will be maintained in EIS support. GSA benefits from ECD funded development of 4G LTE enhancements and network modifications to support WPS, as well as future development of 5G enhancements and network modifications. As this occurs, AT&T will make GSA aware of any commercial carrier service changes that may impact WPS functional capabilities and user operational concerns.

Did You Know?

Following September 11, 2001, AT&T participated in the development of WPS Industry Requirements under auspices of the ECD, and implemented and deployed WPS at Full Operating Capability (FOC) for Global System for Mobile (GSM)-based systems in 2004.

AT&T Mobility supports NS/EP critical users' needs for priority wireless call processing that is fully integrated with wire line priority treatment in the AT&T NS/EP services. With AT&T WPS, ECD-approved critical users (subscribed to on a per cell phone basis) receive priority access and processing by dialing the *272 feature code with the destination number, which enables priority access call queuing to the radio traffic channel and network trunks during congestion situations. If an NS/EP call is received by the Session Border Controller (SBC)/ Proxy-Call Session Control Function(P-CSCF) (whether the call was WPS initiated or GETS initiated) and is destined to a mobile subscriber on the system, the call will receive priority handling towards the destination/terminating number.

As requested by ECD/DHS, AT&T WPS uses an industry-modified enhanced Session Initiation Protocol (SIP) Resource Priority Header (RPH) specification to support priority capability within WPS network. SIP RPH supports five levels of priority.

With DHS/ECD support, AT&T recently implemented LTE capabilities further extending WPS callers' priority during emergencies. Adding features such as Automatic Access Class Barring, High Priority Access Treatment, and Paging Priority Treatment and Differentiation, AT&T WPS users have the highest probability of connection and completion of their wireless NS/EP calls. Enhancements to provide for operations within future mobility technology such as 5G are already being planned.

H-3.3 Telecommunication Service Priority [G.11.3.3]

TSP is a program mandated by the Federal Communications Commission (FCC), which establishes the legal basis for telecommunications vendors to act on a priority basis in order to initiate, restore, or otherwise act on a priority basis to confirm effective NS/EP telecommunication services. We currently execute this process for NS/EP and understand how to maintain full capability and compatibility with EIS TSP needs. Agencies are able to request TSP treatment for any service that is uniquely identifiable and provided in support of a customer's NS/EP mission. Agencies obtain a TSP authorization code from the Office of Priority Telecommunications (OPT), which is valid for a period of three years. Agencies must request TSP restoration priority before an outage occurs. Full TSP restoration services and management are described in this section to show our understanding and capabilities.

TSP is applicable to all aspects of end-to-end telecommunication services including: dedicated private lines; access lines; dial-tone lines; high-capacity digital systems; trunks between another carrier's switched network; or wireless nodes and priority as required for design change of circuits, including coordination between local access providers and the transport segment.

Agencies with TSP requirements are supported by a dedicated team at the AT&T Customer Care Center and office of the TSP coordinator to provide enhanced oversight of all TSP orders. **Figure H-2** provides a glimpse of our AT&T Network Operations Center that has established TSP status and resolution tracking into our global network management systems. AT&T follows the TSP allowance for five levels of priorities for restoration and provisioning of TSP services. Restored circuits retain the property (i.e., TSP levels) of the original circuit. Agencies' orders with TSP provisioning priority codes

are provided their respective priority by TSP expeditors within the AT&T Government Customer Care staff.

To provide faster and more reliable TSP provisioning, a dedicated team of professionals mobilize when TSP order requests are received. TSP orders generally require manual coordination, especially during hours outside the normal business day. In these

circumstances, enhanced oversight is provided by the

AT&T Government Customer Care Center and coordinated with the affected access service providers. To verify that TSP provisioning orders receive priority outside the normal business hours, identified expeditors are included in the TSP Point of Contact (PoC) list. Maintenance technicians work TSP trouble tickets before working on any other trouble tickets, handling them in the proper TSP restoration priorities.

Maintenance technicians' managers verify that tickets with a TSP code are given top priority over non-TSP circuits. Restoration of service with TSP restoration priority is enhanced by our self-healing network, in conjunction with processes built into AT&T OSSs (Operations Support Systems) and special handling by AT&T Government Customer Care staff as indicated by the following features:

- The self-healing network resiliency features residing within our network architecture automatically reroute services from the damaged facility to spare capacity in operating facilities. Customers are often unaware of damage to our network because of AT&T self-healing network capabilities.
- The AT&T Fast Automatic Restoration (FASTAR) capability, in conjunction with the Restoration and Provisioning Integrated Design (RAPID) system correlates alarm data from network transport equipment and calculates re-routes based on spare capacity in the transport network. FASTAR controls restoration path implementation and prioritizes the restoration of disrupted T3s based on the Transport Service Now (TSNOW) system-ranking algorithm. The T3s carrying TSP circuits are given a priority restoration over T3s without TSP services.
- TSP is incorporated in AT&T key maintenance systems. Process methods and procedures are written into our manuals and built directly into our OSSs. As a result,



Figure H-2. AT&T Worldwide Control Center.

priority handling is achieved without manual invocation. For example, if a facility fails because of a cable cut, our OSSs use TSP indicators in computing the priority of automatic restoration. For other types of failures, once a customer detects and reports trouble on a TSP labeled circuit, the OSSs automatically identify and highlight those tickets in order to place them to the top of the list for testing and dispatch, even without an agency explicitly stating that TSP is applicable to that circuit. TSP is a key consideration driving AT&T restoration process from the repair center, to the central office, to the dispatch center.

- Throughout AT&T, customer service personnel are trained to provide priority treatment to TSP-designated circuits.

Agencies have resilient and robust telecommunications services because AT&T tracks all facility and equipment failures and assesses their impact on customer service. When an event exceeds established thresholds of duration, severity, or service impact, our Command, Control, and Communications Program (3CP) incident management process is activated. Through 3CP processes supported by the AT&T Technical Control Bridge (TCB) and Management Control Bridge (MCB), all AT&T organizations are represented at the appropriate level of management oversight to respond to the incident and restore service as rapidly as possible. TSP is factored into these actions whether they are manually or automatically executed. These processes are triggered even in the event of a failure that might not impact customers. At the conclusion of the event, post-incident analysis is undertaken to resolve any shortcomings and plan for future incidents and recommend any mitigation options to ECD.

AT&T supports TSP requirements and fully complies and interoperates with any future commercially available TSP replacement system.



General Services Administration (GSA)

Office of Information Technology Category

Enterprise Infrastructure Solutions (EIS)

GS00Q17NSD3000

Appendix I — Assumptions and Conditions



APPENDIX I — VOLUME 2 ASSUMPTIONS AND CONDITIONS [L.9]

I-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 I-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, AT&T takes no exceptions or deviations from the government's requirements, clauses, provisions or terms and conditions of the RFP.

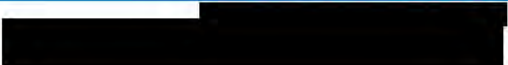
Table I-1-1. Volume 2 — Assumptions and Conditions.



#	Assumption or Condition	Area of the Proposal Affected	Area of the RFP Affected	Discussion	Resolution

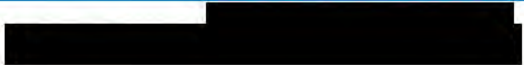


#	Assumption or Condition	Area of the Proposal Affected	Area of the RFP Affected	Discussion	Resolution





#	Assumption or Condition	Area of the Proposal Affected	Area of the RFP Affected	Discussion	Resolution





#	Assumption or Condition	Area of the Proposal Affected	Area of the RFP Affected	Discussion	Resolution

