

2.3.13 Operational Support Systems [L34.2.3.13], [C.3.9.2.2]

The Government and its Customer Agencies can efficiently manage their operations and reduce costs through use of integrated Operational Support Systems (OSS) combined with an award winning web portal to handle their daily tasks.

The offeror shall describe its overall approach to Operational Support Systems (OSS) to support billing, service ordering, customer support, service management, inventory management, and program management, as required by Section C.3.9, Operational Support Systems, and Section E, Inspection and Acceptance.

Overview

GSA and Agencies fulfill their critical missions through the use of integrated Operational Support Systems (OSS) supported by AT&T Government Solutions. These support systems provided by AT&T, a full service provider, are integrated into our overall [REDACTED] and provide the flexibility needed to implement Government requirements. The systems are designed to provide Networx users with a positive experience for ordering, billing, inventory management, service management, customer support, and overall program management. For ease of use, GSA and Agencies are provided with the ability to perform their key functions through a single secure entry point. The award-winning [REDACTED] secure web portal allows customers access to an entire suite of systems 24x7, providing the benefit of greater control of their services, any time, any place. This portal currently supports [REDACTED] annually and is used by existing Government and commercial customers. Using this tool, GSA and Agencies experience a wealth of information just a 'click' away; yet should they need direct contact, the Customer Support Office (CSO) within the Contractor's Program Organization (CPO) is available at 1-877-GET-NTWX.

██████████ AT&T's customer support, service, and management web portal, has been awarded a 2004 Innovation Award from TMC Labs.



"AT&T is setting new standards for network management, customer service and support applications with AT&T BusinessDirect," TMC President Rich Tehrani.



As shown in ██████████ a single portal for service ordering, service management, inventory management, trouble ticketing, billing, customer support, and program management provides the Government with the ability to perform the functions in ██████████

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

Unlike our competitors who have been distracted by internal financial concerns,

[REDACTED]
[REDACTED]
[REDACTED]

AT&T is unique in our ability and willingness to invest in the technology needed to provide the Government features and benefits shown in


[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]



GSA and Agencies benefit from our continuing investment in core network technology and OSS. One of the key OSS investments is the [REDACTED]



Service	Percentage
Online banking	95%
Mobile banking	85%
Online bill payment	90%
Online account opening	100%
Online loan application	98%
Online investment services	92%
Online insurance services	88%
Online credit card services	96%

[REDACTED]

[illegible]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Billing

GSA and Agencies are provided the best customer billing solution in the industry through efficient billing support tools and systems and an experienced Networkx team serving Government customers. Delivering accurate and timely Networkx billing data is an absolute necessity and represents the primary objective of the Networkx billing team. However, rendering high quality invoices on time is just the beginning. Invoices must be presented in a format allowing Federal customers to fully view, manipulate, and process the data as efficiently as possible. [REDACTED]

[REDACTED], support from an experienced CSO and a dedicated CPO focused on the complete success of Networkx make the billing experience complete.

From the original FTS2000 contract to the current FTS2001 Crossover contract, a long history has demonstrated our support for billing requirements of Federal Customer Agencies. From a billing perspective, the [REDACTED] portal is the launching point to other applications performing the following tasks:

- Provide total access to billing information in a secure, web-based environment
- Fully support direct billing, centralized billing, and shared tenant billing

- Allow Government users to quickly and easily submit, track, and get resolution to billing inquiries and disputes
- Permit Networkx users to cross-reference Agency Hierarchy Codes (AHCs) to AT&T internal accounting information
- Provide access to an online pricing tool to use for cross verification of Networkx billed charges

One of the applications available through [REDACTED] [REDACTED] which allows Networkx customers to have a web-based view of the data produced by the [REDACTED] has the ability to take billing data for multiple Networkx services and combine it onto a single, easy- to-interpret invoice. [REDACTED] is available for Government customers today and will be further enhanced to meet all of the new billing requirements for Networkx. It has the ability to provide control over how they view, analyze, sort, and manage billing data for multiple services. [REDACTED] has the unique capability to receive data feeds from multiple systems, including the Networkx subcontractor's operating systems. This data is aggregated onto a single invoice inclusive of all Networkx charges. This includes the capability of clearly displaying any Service Enabling Device (SED) and associating it with the service its supports.

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

The [REDACTED] provides GSA and [REDACTED] Agencies with Networx billing data [REDACTED] that consistently exceeds GSA [REDACTED] requirements. Some of the features [REDACTED] and benefits associated with [REDACTED] are listed in [REDACTED]

Government customers experience the following benefits with the [REDACTED] [REDACTED] option:

- Manage AT&T bills conveniently and securely, 24x7
- View the current Networx bill and 12 previous months bills online
- Analyze bills conveniently online with many different standard or custom reports
- Save time by minimizing phone calls and callbacks
- Submit billing inquiries, disputes, and track them through to resolution
- Decrease manual entries/improve transaction accuracy
- Cut costs by increasing productivity and redirecting resources
- Gain hands-on control of billing with up-to-the-minute status
- Eliminate paper bills
- Confidently rely on industry leading security practices
- Gain access to billing information on demand
- Validate and authorize Customer Agency personnel

If, for any reason, the Agency has questions on their invoice, they can enter queries through the [REDACTED] web portal by selecting [REDACTED] [REDACTED] From there, they can click on [REDACTED] [REDACTED] GSA and Agency users can drill down to individual charge level items and submit their query/dispute with a few clicks of the mouse. The [REDACTED] [REDACTED] tool automatically brings up the disputed charges along with much

of the charge level information pre-populated to reduce the amount of input required by Agencies. Networx customers can also benefit by accessing the [REDACTED] to create ad hoc reports, customized to meet individual Agency or GSA needs.

Service Ordering

GSA and Agencies are fully supported with a powerful set of secure service order management tools used to submit service orders easily and track orders through to completion. Over the past two decades, [REDACTED] [REDACTED] to successfully support large Federal contracts, such as FTS2000 and FTS2001 Crossover. AT&T is recognized as a major telecommunications provider to the Government and we continuously strive to enhance their service ordering experience.

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

We facilitated the creation of easy to use tools and processes, and GSA and Agencies are provided with secure, convenient, electronic order management resources to simplify order issuance, tracking and receipt of acknowledgement and confirmation notices. These functions can be performed on line, reducing time spent on paperwork and telephone calls. Currently, over [REDACTED] annually go through the web portal that is used today by FTS 2001 Crossover customers and by AT&T's largest commercial customers. Government customers can perform the service order functions listed in [REDACTED]

GSA and Agencies can also fully manage who accesses information and the level of access provided. For example, an Agency may want to establish

[REDACTED] permissions that allow users to submit orders but not to view and download bills. The [REDACTED] Agency Administrator (often the Designated Agency Representative (DAR) Administrator) can set up this type and other types of access control as shown in [REDACTED]

[REDACTED]

[REDACTED]

Government customers may submit orders electronically using the [REDACTED] [REDACTED] web portal. This allows Networkx customers to perform the ordering functions listed in [REDACTED]

Government customers who choose not to submit or track orders electronically can rely on the highly trained personnel within the CSO to provide ordering support.

When a Government customer is preparing to issue orders, the customer's existing inventory is retrieved, whenever possible. Several online fields are pre-populated with the customer's data, such as name, address, contact information, service type, and circuit identifier. Once again, this eliminates the need for Networkx customers to re-key common information. The benefits of Government ordering are:

Government Ordering Benefits

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Pages 388 and 389 intentionally left blank.



Customer Support

The Networkx CSO is established organizationally with proven processes, robust systems and efficient tools dedicated to support the Networkx requirements. AT&T is revamping all aspects of the customer experience in the telecommunications industry by simplifying Service Level Agreements (SLAs), slashing cycle time, improving accuracy, and rolling out powerful electronic servicing capabilities. All of this revamping translates into Government benefits for trouble and complaint handling, queries, technical support, revenue forecasts, service optimization, billing, training, and ordering.

[REDACTED] for Networkx is provided by AT&T Government Solutions, a business unit of AT&T. Networkx Subscribers have easy access to support systems in one common area, through the [REDACTED] web portal, as shown in [REDACTED]. Designed to give Networkx users greater control of communications from any location, worldwide, 24x7, GSA and Agencies have easy access to [REDACTED].



Service Management

The critical nature of Government missions depend on the capability to operate and manage Networkx services to the level of performance required. GSA and Agencies can be assured that AT&T's management solution is built upon reliability and performance with Networkx tailored systems, processes and professional staff support provided by the CPO.

The components of the system architecture used to support Networkx services, the associated functions, and GSA Customer Benefits are described in [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]		

[REDACTED]

These architectural components represented in [REDACTED] provide GSA Customers with demonstrable [REDACTED] and are accessed through a secure web portal that provides visibility to track service quality. In addition, [REDACTED]

[REDACTED] shows a common database and services [REDACTED] The database of record is a single common database for each element of the GSA Customers' service.

[REDACTED]
[REDACTED]
[REDACTED]

As shown in [REDACTED] [REDACTED]
[REDACTED] is a secure portal for complex user requirements and service

"With all the communication services and equipment that must be tracked and paid for, (government) agencies are also demanding that telecommunication service providers offer ways to make their management chores easier. For instance, more than a dozen agencies are using [REDACTED] which allows them more control over the networks AT&T manages for them. Agencies can get a nationwide view of their networks and how they are working."

management.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

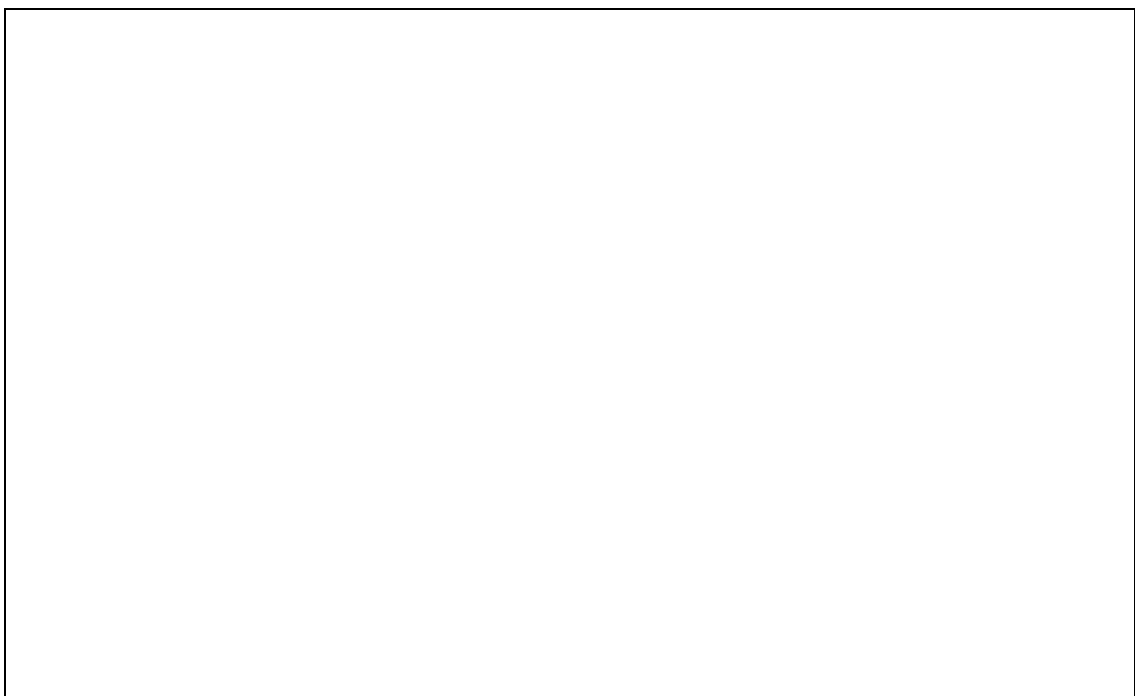
[REDACTED]

[REDACTED]

These tools combined with the support of the CPO, are provided to help GSA and Agencies spend more time on critical missions.

Inventory Management

GSA and Agencies receive accurate, up-to-date Networkx inventory information, simply accessed through a secure web portal. By selecting [REDACTED] [REDACTED] as shown in [REDACTED], Networkx inventory is effectively managed and maintained.





Government customers can view accurate and current inventory data for its management needs whenever required. Agencies with multiple and complex requirements are able to take advantage of securing inventory data from a single source for all Networkx services. Consequently, the Government saves time and gains productivity as Agencies select and procure Networkx services.

Service Order Completion Notices (SOCNs) are delivered to the Government electronically, as specified in Section C.3.5 of the RFP, Service Ordering, and defined in Section J.12 of the RFP, Ordering and Billing Data Elements. All the data elements listed on the SOCN are maintained and updated, as required, in the [REDACTED] database. As a final step of the order completion process, shown below in [REDACTED] the Networkx [REDACTED] [REDACTED] database is updated within 24 hours of posting the SOCN. This timely update also allows the Government to use the Networkx [REDACTED] [REDACTED] to verify service orders and transition completions.



Updates to the inventory are driven by service orders. Therefore, changes to the service, such as added features, replacement of service enabling devices (SEDs), or disconnects, are recorded in the [REDACTED] [REDACTED] database, from data in the SOCN for the service order. The ability to

verify and track all service changes and updates to the inventory database within the same inventory system tool is extremely helpful and convenient in verifying data and resolving inventory discrepancies or billing inquiries.

The [REDACTED] enables the user to create an inventory report [REDACTED] [REDACTED] of interest as applicable. For example, the user can create a list of [REDACTED] [REDACTED] This report could be further [REDACTED] This flexibility [REDACTED] is designed so the Government can work more efficiently with the resulting reports and their assigned tasks.

- The [REDACTED] view of the Networkx [REDACTED] [REDACTED] contains [REDACTED] which provides a list of [REDACTED] for [REDACTED] When a single inventoried service is being viewed online, the Government user can click on the [REDACTED] [REDACTED] link to [REDACTED]. This information, conveniently accessed in the Networkx [REDACTED], is

essential for [REDACTED]. The Government can expect efficiency and productivity to increase with use of the Networx [REDACTED].

Program Management

For Networx, [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] have been in existence since 2000 and are familiar systems to FTS2001 Crossover customers.

The specific systems tailored for Government use are all available via [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

These systems further refine our approach of [REDACTED]
All these systems handle the entire suite of Networx services. This eliminates the confusion often occurring when an Agency receives bills out of multiple billers from a single vendor. Although the Networx RFP allows multiple billers to be utilized, [REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

OSS Integration

The offeror shall describe its degree of integration among all OSS.

AT&T has tailored our commercial “Target Architecture” to meet Government and Networx requirements. GSA and Agencies are provided with the ability to perform their key functions through access to a secure, web portal interface which allows Government customers access to an entire suite of applications, 24x7.

These customer support management applications and tools are accessible through the [REDACTED] portal. GSA and Agencies can easily and securely share information, [REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED] presents the applications offered to GSA and Agencies to manage their Networkx services. This information, accessible via a single logon ID in the [REDACTED] portal sets the pace and [REDACTED] [REDACTED] by offering the most complete and well integrated presentation of Government and Networkx information.

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]



Category	Value
Category 1	Value 1.1
Category 2	Value 2.1
Category 3	Value 3.1
Category 4	Value 4.1
Category 5	Value 5.1
Category 6	Value 6.1
Category 7	Value 7.1
Category 8	Value 8.1
Category 9	Value 9.1
Category 10	Value 10.1
Category 11	Value 11.1
Category 12	Value 12.1
Category 13	Value 13.1
Category 14	Value 14.1
Category 15	Value 15.1
Category 16	Value 16.1
Category 17	Value 17.1
Category 18	Value 18.1
Category 19	Value 19.1
Category 20	Value 20.1
Category 21	Value 21.1
Category 22	Value 22.1
Category 23	Value 23.1
Category 24	Value 24.1
Category 25	Value 25.1
Category 26	Value 26.1
Category 27	Value 27.1
Category 28	Value 28.1
Category 29	Value 29.1
Category 30	Value 30.1
Category 31	Value 31.1
Category 32	Value 32.1
Category 33	Value 33.1
Category 34	Value 34.1
Category 35	Value 35.1
Category 36	Value 36.1
Category 37	Value 37.1
Category 38	Value 38.1
Category 39	Value 39.1
Category 40	Value 40.1
Category 41	Value 41.1
Category 42	Value 42.1
Category 43	Value 43.1
Category 44	Value 44.1
Category 45	Value 45.1
Category 46	Value 46.1
Category 47	Value 47.1
Category 48	Value 48.1
Category 49	Value 49.1
Category 50	Value 50.1
Category 51	Value 51.1
Category 52	Value 52.1
Category 53	Value 53.1
Category 54	Value 54.1
Category 55	Value 55.1
Category 56	Value 56.1
Category 57	Value 57.1
Category 58	Value 58.1
Category 59	Value 59.1
Category 60	Value 60.1
Category 61	Value 61.1
Category 62	Value 62.1
Category 63	Value 63.1
Category 64	Value 64.1
Category 65	Value 65.1
Category 66	Value 66.1
Category 67	Value 67.1
Category 68	Value 68.1
Category 69	Value 69.1
Category 70	Value 70.1
Category 71	Value 71.1
Category 72	Value 72.1
Category 73	Value 73.1
Category 74	Value 74.1
Category 75	Value 75.1
Category 76	Value 76.1
Category 77	Value 77.1
Category 78	Value 78.1
Category 79	Value 79.1
Category 80	Value 80.1
Category 81	Value 81.1
Category 82	Value 82.1
Category 83	Value 83.1
Category 84	Value 84.1
Category 85	Value 85.1
Category 86	Value 86.1
Category 87	Value 87.1
Category 88	Value 88.1
Category 89	Value 89.1
Category 90	Value 90.1
Category 91	Value 91.1
Category 92	Value 92.1
Category 93	Value 93.1
Category 94	Value 94.1
Category 95	Value 95.1
Category 96	Value 96.1
Category 97	Value 97.1
Category 98	Value 98.1
Category 99	Value 99.1
Category 100	Value 100.1

Use of a single portal for service ordering, service management, inventory management, trouble ticketing, billing, customer support and program management provides the Government with the ability to:

- Improve order accuracy by [REDACTED]
[REDACTED]
- Shorten provisioning intervals [REDACTED]
[REDACTED]
- [REDACTED] information through [REDACTED]

[illegible]

- Save administration time by [REDACTED]
[REDACTED]
- [REDACTED] without needing to contact the Customer Support Office (CSO) for inquiries

Verification Testing

In addition, the offeror shall address its OSS approach to:

(a) Verification Testing

With the critical nature of the Government's missions, it is imperative the [REDACTED] be ready for GSA and Agencies, [REDACTED]

[REDACTED]
This is demonstrated through achievement of the OSS Verification Test objectives [REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED] It can then be [REDACTED]. GSA and Agencies are shown that all OSS for service ordering, billing and inventory management tools (essential to providing the Networx services) are in place and fully operational.

Government-provided data, if requested, is used for the OSS Verification Test. The Government and the Networx team work together to establish an acceptable test plan. [REDACTED]
[REDACTED]



When a new service is offered, the Test and Turn Up process will demonstrate that services are operational and Key Performance Indicators (KPIs) /Acceptable Quality Levels (AQLs) are met. This is coordinated through the CPO and the Government may participate or observe the test.

Further detail is provided in Section 2.3.13.1 and in the Networkx OSS Verification Test Plan (Appendix F).

Security and Performance

(b) Security and Performance

In order to meet critical Government security requirements,

[REDACTED]

[REDACTED]

The Networkx security approach includes the following:

[REDACTED]

To accomplish Government goals, tasks for the AT&T Networkx Team are shown below:

[REDACTED]

Further detail is provided in Section 2.3.13.2 and in the Networkx Security Plan in Appendix C.

Change Control

(c) Change Control

OSS need to be adaptable to change, especially with the rapid pace of IT convergence. GSA and the Agencies are provided with systems [REDACTED]

[REDACTED]

[REDACTED] This process protects Government information by [REDACTED]

[REDACTED] The Change Management Plan (Appendix G) provides details of [REDACTED]

Government coordination and communication for OSS changes will be accomplished through the OSS [REDACTED]

[REDACTED] The Government is able to easily obtain change information and when the changes are implemented.

Further detail is provided in Section 2.3.13.3 and in the Networx Change Management Plan in Appendix G.

The offeror shall provide an OSS Verification Test Plan, in accordance with Sections C.3.9.2.2, Step 2, Verification Testing; E.2, Verification Test Plans; and E.3, Verification Testing of Contractor's Operational Support Systems. The offeror shall describe its OSS security as part of the Security Plan required in Section L.34.2.3.3, Security Management. The offeror shall describe its OSS change control in an OSS Change Management Plan as required in Section C.3.9.2.3, Step 3, Change Control.

AT&T has provided the required plans in the Appendix reference in **Table 2.3.13-10**.

PLAN	APPENDIX LOCATION	REFERENCES
OSS Verification Test Plan	F	C.3.9.2.2, Step 2, E.2., E.3
Security Plan	C	L.34.2.3.3
OSS Change Management Plan	G	C.3.9.2.3, Step 3

Table 2.3.13-10: Appendix References. AT&T has supplied the Appendix where GSA will find the required plan.

The contractor shall provide an OSS Verification Test Plan, in accordance with Section E, Inspection and Acceptance at contract award. [C.3.9.2.2]

The OSS Verification Test Plan (Appendix F) outlines the details of the test in accordance with Section E, Inspection and Acceptance. This test serves to verify

OSS are in place, operational, using Government provided data when requested.

2.3.13.1 Verification Testing [L.34.2.3.13.1], [E.2], [E.2.1], [E.2.2]

The offeror shall describe its approach to provide OSS verification testing.

The offeror shall address the following at a minimum:

- (a) Completeness and consistency of its plan for meeting the requirements of Section E, Inspection and Acceptance and meeting all performance requirements
- (b) Testing approach which supports completion of testing within 60 calendar days from the Notice to Proceed or the date GSA approves its OSS Verification Test Plan (whichever is later), even if any retesting is required, with a description of how Government observers are involved
- (c) Effective and timely testing for new functionality or services

GSA and Agencies will have fully operational OSS ready to order Networkx services. [REDACTED]

[REDACTED]

[REDACTED] AT&T follows the guidelines in Section E: Inspection and Acceptance, for the OSS Verification Test Plan and the Networkx Services Verification Test Plan, and the execution of the associated tests to meet the testing and performance requirements.

For Networkx, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] This coupled with an [REDACTED] [REDACTED] serves to validate completeness and accuracy of the OSS. The

[REDACTED] is used as products/services and changes are introduced into the existing OSS. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The Networkx [REDACTED]
[REDACTED]

Once the Networkx OSS Verification Test Plan is approved by GSA, the test begins. AT&T utilizes the test data provided by the Government to ensure the outcome meets the pre-defined expected results. This test verification process provides GSA and Agencies with the confirmation all OSS are in place and are fully operational. This is demonstrated by using Government data to:

- Accept and process orders and produce acknowledgements
- Process bulk orders
- Produce billing files
- Verify that orders update inventory correctly
- Provide proper security and authorization for access

This test is coordinated using a preplanned schedule and is completed within 60 days of Notice to Proceed or the date GSA approves the OSS Verification Test Plan, depending on which date occurs later. Results of the test are recorded and reported to the GSA Contracting Officer's Representative

(COR). [REDACTED]

[REDACTED] however, no Networx orders are processed until approval is given by the Government.

Data and Interfaces

(d) Complete description of data and interfaces

Using data provided by the Government, the OSS Verification Test is used to validate the readiness of the OSS and the ability to:

- Accept and process orders and produce acknowledgements
- Process bulk orders
- Produce billing files
- Verify orders update inventory correctly
- Provide proper security and authorization for access

[REDACTED] shows the [REDACTED]

Networx and the OSS Verification Test.



[REDACTED]

[REDACTED] below describes in more detail how [REDACTED]

[REDACTED] to meet the requirements of the OSS Verification Test.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

I [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

I [REDACTED]

[REDACTED]

[REDACTED]

I [REDACTED]

[REDACTED]

[REDACTED]

(e) Meeting of test results reporting requirements

When the Networkx OSS Verification Test begins, the OSS Verification Test Results Report (Appendix F, [REDACTED]) initiates progress tracking and recording. This report lists the Networkx services, as specified in Section C.2, and [REDACTED]

[REDACTED] The report is available in the media types specified in C.3.9.4.1.2.3, Media/Transport/Format – OSS Verification Test Results and are delivered to the GSA COR within five business days of completion of the tests.

The contractor shall develop and execute a Networkx Services Verification Test Plan to verify that the services delivered under the contract meet the requirements of Section E.4, Verification and Acceptance Testing of Networkx Services, and shall develop and execute an OSS Verification Test Plan to verify that its OSS meets the requirements of Section E.3, Verification Testing of the Contractor's Operational Support Systems. [E.2]

A Networkx Services Verification Test Plan to verify that the services delivered under the contract meet the requirements of Section E.4, Verification and Acceptance Testing of Networkx Services will be developed and executed by AT&T. Further detail will be provided in the Networkx Services Verification Test Plan which will be delivered as specified in Section F, ID 95, within 60 calendar days after the Notice to Proceed. The Networkx Services Verification Test Plan and OSS Verification Test Plan are located as shown in **Table 2.3.13.1-2**.

PLAN	APPENDIX LOCATION	REFERENCES
Networkx Services Verification Test Plan	To be delivered 60 days after Notice to Proceed	C.2, E.2.2,E.4
OSS Verification Test Plan	F	E.2.1, E.3

Table 2.3.13.1-2: Appendix References. *AT&T has supplied the Appendix where GSA will find the required plans.*

The contractor shall prepare an OSS Verification Test Plan in accordance with the requirements of Section C.3.9, Operational Support Systems, and Section E.3, OSS Verification Testing of the Contractor's Operational Support Systems. The contractor shall update the OSS Verification Test Plan when a new service is offered or when an OSS is changed. [E.2.1]

The OSS Verification Test Plan (Appendix F), prepared in accordance with Section C.3.9., Operational Support Systems and Section E.3, Operational Support Systems (OSS) Verification Testing of AT&T's Operational Support Systems, outlines the details of the test. This test demonstrates to GSA and Agencies that all OSS are in place to meet the Networkx requirements. When a new service is offered or when the OSS is changed, AT&T will update the OSS Verification Test Plan (Appendix F).

This page intentionally left blank.

The test cases that the contractor shall execute acceptably include those listed in Table E.3.1. [E.3]

The Network OSS Verification Test test cases will be executed acceptably in accordance with the test cases listed in Table E.3.1. and shown in





The contractor shall demonstrate acceptable performance using one of the following electronic media: Internet secure access, electronic mail, or electronic file transfer. [E.3]

The Network Services Verification Test results and OSS Verification Test results are demonstrated using the media types required by the Government: Internet secure access, electronic mail or electronic file transfer.

2.3.13.2 Security and Performance [L.34.2.3.13.2, C.3.9.2.1]

The offeror shall describe its approach to provide OSS security

In today's world, more than ever before, it is imperative for GSA and Agencies to maintain a secure operating environment. AT&T is deeply committed to a rigorous practice of discipline around security, and commitment is embedded throughout all processes, from desktop management to network and service security. Government customers benefit from the approach, governed by deep security expertise, which exemplifies

the due diligence and discipline a service provider can use to implement leading practices to protect its computing infrastructure.

[REDACTED]

For each new service or feature, the [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] begins with establishment of a security plan. [REDACTED]

[REDACTED] The responsible organizations and contacts are listed, including points of contact for the Government. Systems are assigned a status of: [REDACTED]

[REDACTED] A description of the Networx program is provided along with [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Government information has a high level of sensitivity and requires protection. AT&T recognizes this as one of the [REDACTED]

[REDACTED] for Networx. Based upon this [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Management controls are [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

An OSS Security Plan can be developed at any point in [REDACTED]
however [REDACTED]
[REDACTED] There
are [REDACTED]

[REDACTED]

[REDACTED]

--

[REDACTED]

Operational Controls

To further protect GSA and Agencies, [REDACTED] shown in [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[illegible]



1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7
8	8	8
9	9	9
10	10	10
11	11	11
12	12	12
13	13	13
14	14	14
15	15	15
16	16	16
17	17	17
18	18	18
19	19	19
20	20	20
21	21	21
22	22	22
23	23	23
24	24	24
25	25	25
26	26	26
27	27	27
28	28	28
29	29	29
30	30	30
31	31	31
32	32	32
33	33	33
34	34	34
35	35	35
36	36	36
37	37	37
38	38	38
39	39	39
40	40	40
41	41	41
42	42	42
43	43	43
44	44	44
45	45	45
46	46	46
47	47	47
48	48	48
49	49	49
50	50	50
51	51	51
52	52	52
53	53	53
54	54	54
55	55	55
56	56	56
57	57	57
58	58	58
59	59	59
60	60	60
61	61	61
62	62	62
63	63	63
64	64	64
65	65	65
66	66	66
67	67	67
68	68	68
69	69	69
70	70	70
71	71	71
72	72	72
73	73	73
74	74	74
75	75	75
76	76	76
77	77	77
78	78	78
79	79	79
80	80	80
81	81	81
82	82	82
83	83	83
84	84	84
85	85	85
86	86	86
87	87	87
88	88	88
89	89	89
90	90	90
91	91	91
92	92	92
93	93	93
94	94	94
95	95	95
96	96	96
97	97	97
98	98	98
99	99	99
100	100	100

[REDACTED]

Technical Controls

The OSS used by GSA and Agencies are further protected by [REDACTED]
[REDACTED] shown [REDACTED] which [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[illegible]

Lastly, the [REDACTED] specifies details regarding how the Government is [REDACTED] at

The offeror shall include in its Security Plan its methods for meeting the requirements of Section C.3.9.2.1, Step 1 -- Security and Performance, ID numbers 1 through 3.

The Security Plan is located as shown in **Table 2.3.13.2-4**.

PLAN	LOCATION	RFP REFERENCE
Security Plan	Appendix C	C.3.9.2.1, Step 1, ID Numbers 1-3

Table 2.3.13.2-4: Appendix Reference. *AT&T has supplied the Appendix where GSA will find the required plan.*

The offeror shall address the following at a minimum:

- (a) Complete description of methods to ensure implementation of auditability, access controls, data protection, and backup and recovery of the OSS

Auditability

GSA and Agencies can be assured a level of technical security exists to protect the system from identified vulnerabilities. [REDACTED]



A horizontal bar chart consisting of 25 black bars. The bars are arranged in five groups of five. The first group (top) has the longest bars, with the first bar being the longest overall. The second group has bars of slightly decreasing length. The third group has bars of similar length to the second. The fourth group has bars of slightly decreasing length. The fifth group (bottom) has the shortest bars, with the last bar being the shortest overall. The bars are all solid black and have a uniform thickness.

[REDACTED]

[REDACTED]

Lastly, audit logs [REDACTED]

[REDACTED]

Access Controls

The Government receives [REDACTED]

[REDACTED]

These [REDACTED] shown in [REDACTED] below, [REDACTED]

[REDACTED]

[REDACTED]

OSS Access Controls

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The following information was obtained from the review of the records of the Department of Social Services, Division of Child Welfare, dated July 1, 1964:

Data Protection

Government data and systems have a high level of sensitivity and require protection. The information and data stored within, processed by or transmitted through is one of the major risk factors. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] OSS [REDACTED]

Backup and Recovery

[REDACTED], GSA and Agencies can be assured [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Data Integrity Assurance

(b) Methods of assuring data integrity for all stakeholders

The priority of protecting Government data from vulnerabilities i [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



The contractor shall ensure security requirements are met for all automated operational support systems, and shall support Government certification and accreditation of the system via services such as Managed Tier Security Service, Customer Specific Design and Engineering Services, or other services the Government may order to achieve this. The security requirements are defined in Section C.3.3.2, Security Management, and include, at a minimum, security controls for low impact systems as defined in NIST SP 800-53, Annex 1. [C.3.9.2.1]

The OSS used by the Government are [REDACTED]
[REDACTED] in the Security Plan (Appendix C)
and in the overall Security approach. [REDACTED]

AT&T will support the Government in the Certification and Accreditation of the system via services such as Managed Tier Security Service, Customer Specific Design and Engineering Services, or other services the Government may order to achieve this.

The contractor shall describe its methods for securing these systems as part of the overall Security Plan. [C.3.9.2.1]

Each system shall meet the requirements addressed elsewhere in this contract such as security management, fault management, and trouble handling. [C.3.9.2.1]

The Networx OSS used for security management, fault management and trouble handling follow the same security approach and controls as what is outlined in the Security Plan

(Appendix C). As show in



[REDACTED]

[REDACTED]

[REDACTED]

2.3.13.3 Change Control [L.34.2.3.13.3], [C.3.9.2.3]

The offeror shall describe its approach to provide and maintain OSS change control.

Over the life of the Networx contract, changes to the OSS will be required. These changes could be design changes, system upgrades or changes due to system maintenance. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] The process shown in
[REDACTED] begins with a change (add/update/delete) which has been
[REDACTED]
[REDACTED]
[REDACTED]

The Change Management [REDACTED]:

[Redacted content]

The offeror shall include its OSS Change Management Plan for the process of managing changes to OSS according to C.3.9.2.3, Step 3 -- Change Control.

An OSS Change Management Plan (Appendix G) details the Change Management process. [Redacted content]

[Redacted content]

process. These industry recognized standards guarantee GSA and the Agencies interface with systems where changes are identified, authorized, managed and controlled.

The offeror shall address the following at a minimum:

- (a) Description of provision for Government review and approval of changes
- (b) Methods to assure functionality of interfaces for changes
- (c) Methods of communicating to the Government of planned and unplanned changes

Due to the importance of OSS changes on the daily operations of the Government, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

GSA and Agencies should expect OSS changes to have minimal impact on their daily operations. Should OSS changes be made in operational areas affecting the Government, such as ordering, billing, maintenance, inventory and other support systems, there are various ways to advise of the changes, planned or unplanned.

[REDACTED]

The contractor shall deliver an OSS Change Management Plan. [C.3.9.2.3]

The OSS Change Management Plan is included in Appendix G.

The OSS change management requirements shall include, at a minimum, how the contractor will conduct the following:

1. Informing the Government when OSS design changes are planned and when maintenance changes are required

In addition to notifying GSA and Agencies through the methods described in

[REDACTED]

this information is communicated with the Government as specified in the Change Management Plan (Appendix G).

2. Managing and controlling OSS changes

OSS changes are managed with the process outlined in the Change Management Plan (Appendix G). [REDACTED]

[REDACTED]

3. Incorporating Government review and approval by the Government into the contractor's change management process

In order to ensure coordination and communication with the Government on OSS changes, [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

4. Government training, if required by the changes

GSA and Agencies must be kept current with methods for utilizing their Networkx systems and tools. Should changes affect the OSS and require Government training, the Change Control process identifies the need. The

[REDACTED]
[REDACTED]

5. Retesting with the Government to ensure functionality of any impacted interface. [C.3.9.2.3]

With a controlled system release process, GSA and Agencies can be assured changes are thoroughly tested at all levels to ensure accuracy and full functionality prior to moving into a production environment. [REDACTED]

[REDACTED]

[REDACTED] described in the Change Management Plan (Appendix G) which outlines the steps followed for managing, testing, approving and controlling the changes.

Summary

The OSS described in this section combine to provide GSA Customers with access to future Networkx services in evolving telecommunications technology. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]