CIO

"How To Open The Kimono Safely – AT&T has used a layered approach to building a secure customer access system"

The ability to segregate allows AT&T to treat customer groups differently, so specific groups would get access to AT&T's systems using different segments of different zones. "Every zone segment has its own intrusion detection, its own application firewall," says Eslambolchi. AT&T protects customer data by providing the authenticated access through HTTPS or SSL, and authorization and encryption vary by customer. "There are different levels of security across the platform," says Eslambolchi, who also subjects the system to what he calls self-inflicted "ethical hacking" to make sure it can withstand hacking attempts by outsiders. ***BY ALICE DRAGOON*** *Feb. 15, 2005*

System Access Controls

The operations interface to network elements and access to operations support systems are provided through a dedicated operations network. [redacted]

Resource Access Controls

Persons with authorized access to operations support systems are restricted to authorized activities by various access control mechanisms, [redacted] AT&T [redacted] AT&T [redacted] Government [redacted] access to **Business**Direct. AT&T works with each Government Agency to establish a "company administrator" for the **Business**Direct IDs. [redacted] Agency [redacted] Agency. [redacted] Agency [redacted] **Business**Direct [redacted]

[redacted]

BusinessDirect [redacted]

Operational Access Controls

Each person with privileged access to a Networx system is granted access based upon assigned responsibilities. Each privileged user's access is restricted to the minimum necessary permissions to perform assigned duties.

[redacted]

The assignment of user privileges follows the Agency's protocols for requesting, establishing, issuing, and closing privileged user accounts. The Networx security manager, implementation or transition project manager, or delegate provides oversight for access requests and approvals. [redacted]

On a regular basis, the AT&T Networx security manager, project manager, or delegate reviews [redacted]

BusinessDirect accounts, by design, are managed directly by the Agency [redacted] by the designated Agency Administrator.

Public Access Controls

PUBLIC ACCESS CONTROLS

When the public accesses the system, additional security controls are used to protect the integrity of the system and the confidence of public access in the system. Such controls include [redacted]

The contractor shall ensure that its access controls provide access to network management or customer-related information only to authorized contractor personnel and Government personnel. [C.3.3.2.2.5]

[redacted]

[redacted] These controls protect the integrity of the system from unauthorized modification of data.

Table 2.3.3.4-1 [redacted] AT&T's [redacted]

AT&T CONTROLS FOR LOGICAL ACCESS	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 2.3.3.4-1: AT&T's Logical Access Management. *Specifically defined access control processes and procedures allows for only authorized permissions.*

The Government and AT&T support staff will have access to the secure Networx web page, through established logical access controls of our secure

web based portal, AT&T **Business**Direct. [redacted]

Denial of Service - The contractor shall adhere, as applicable, to Federal Government accepted security principles and practices per NIST SP 800-14, or better, to protect its transmission facilities, switching components, network management systems and other essential contractor facilities from denial-of-service attacks, intrusions and other perceived threats. [C.3.3.2.2.5]

Employment of a multi-tiered defense solution is used to protect against denial of service attacks, worms, and intrusions. This unique approach places focus for defense on the network rather than edge based security. [redacted] This process allows for a more proactive approach when protecting network services from malicious intruders and unauthorized activities. The ability to be proactive can save critical time in mitigating the adverse conditions before any damage is done and is therefore beneficial to maintaining the Government's services.

"The IP experts said they'd make the network dumb and the end-points smart. What they missed is that it becomes nearly impossible to scale billions of endpoints when you're trying to do encryption and security."

–Hossein Eslambolchi
Former AT&T CTO & CIO
July 2005.

AT&T [redacted] AT&T's [redacted]

[redacted]

Table 2.3.3.4-2 [redacted] AT&T [redacted]

AT&T'S MEASURES TO PROTECT THE SHARED INFRASTRUCTURE
[redacted]
[redacted] AT&T's [redacted]
[redacted]
[redacted]
[redacted] AT&T [redacted]
[redacted]
[redacted] AT&T's [redacted] AT&T [redacted]
[redacted]
[redacted] AT&T's [redacted] AT&T's [redacted]
[redacted]
[redacted] AT&T's [redacted] AT&T certified, wherever appropriate, to the highest industry standards [redacted]
[redacted]
[redacted] AT&T utilizes [redacted]
[redacted]
[redacted] AT&T [redacted] AT&T's [redacted]

Table 2.3.3.4-2: AT&T's Security Measures Protecting Network Infrastructure. *AT&T uses many controls to protect the infrastructure that provides services to the Government.*

In an effort to provide flawless execution of security practices and principles, AT&T Network Security continually probes the various networks, both internally and externally. It deploys an [redacted] AT&T patented technologies to look for potential subversive activity. [redacted]

Implementation of information assurance - The contractor shall describe its protection for information assurance of its databases, OSS, and information systems in its Security Plan. [C.3.3.2.2.5]

Section 6 of the Security Plan (Appendix C) provides a discussion of the security approach and controls. Internal and external access control mechanisms are deployed to limit access to Networx databases and systems as well as support continuous and reliable operations of Networx services.

AT&T will provide protection and information security in accordance with FISMA, NIST SP 800-14, and FIPS PUB 199 and 200 guidelines to prevent the breach of confidentiality, integrity and availability of Networx services. To that end, AT&T will [redacted] AT&T [redacted] Customer Agency's personnel [redacted]

AT&T [redacted] Agency. In addition to these guidelines, AT&T will support the Government [redacted] AT&T.

[redacted] AT&T will implement [redacted] AT&T or Government personnel may [redacted] in accordance with AT&T policy and NIST SP 800-14 guidelines.

AT&T will use [redacted] AT&T's security policy to prevent [redacted]

The contractor shall include in the Security Plan how technicians' accesses and privileges to network elements and routing policies will be controlled and managed. [C.3.3.2.2.5]

The Security Plan (Appendix C) provides a discussion of a logical security approach to assure control of systems by technicians. Logical access controls restricts access to no more functionality than needed to execute an assigned task, i.e., need-to-know. As work is contracted with the Federal Government, and [redacted] and Networx systems become managed, maintained, and/or hosted by AT&T, more detailed information can be obtained to determine appropriate specific accesses and privileges to network elements.

At a minimum, the contractor shall define network elements security policies, access privileges structure, and what processes, procedures, and mechanisms will be in place to control and manage access to network elements and routing policies by contractor's operators and technicians. [C.3.3.2.2.5]

AT&T's Corporate Security organization is [redacted]

AT&T operates in a highly secured environment where physical access to switching centers and other network facilities is strictly monitored and managed. There are well defined policies regarding the security of network elements. These policies define the criteria for securing critical areas and network elements and are applicable to all owned buildings, leased spaces, condominiums and three dimensional conveyance spaces.

Some of the many strategies employed to safeguard assets, and in particular, AT&T's Network are:

[redacted] AT&T facilities [redacted]

[redacted] AT&T's Network Security, [redacted]

[redacted] AT&T's [redacted] AT&T [redacted]

Table 2.3.3.4-3 [redacted] AT&T's Corporate Security [redacted] AT&T's [redacted]

AT&T'S BEST PRACTICES FOR SECURING NETWORK ELEMENTS	
General Policy Considerations	[redacted]

AT&T'S BEST PRACTICES FOR SECURING NETWORK ELEMENTS	
	[redacted]
Assigning Criticality and Protection Levels	[redacted]
Risk Assessment of Physical Access Methods	[redacted]
Assessment of Specific Requirements for the Facilities Include:	[redacted]

Table 2.3.3.4-3: AT&T's Procedures for Securing Network Elements. *This table outlines the areas AT&T's Corporate Security Organization considers when securing switching centers and other network facilities.*

2.3.3.5 Notification of Security Breaches [C.3.3.2.2.6]

The contractor shall take a proactive approach in developing methods to prevent, detect and report security breaches of its network, OSS, and databases. [C.3.3.2.2.6]

A proactive approach to security benefits the Government by preventing and detecting security breaches of [redacted] by creating a security enclave of firewalls and Intrusion Detection Systems. The Government can rely on the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) process managed from the Global Network Operations Center (GNOC) to monitor alarms, data, reports, and intelligence. The C4ISR process puts in place the following functions:

- 24X7 intrusion detection system monitoring

- Data analysis and interpretation
- Incident triage and referral
- Global awareness and facilities.

AT&T MEASURES TO DETECT AND PREVENT SECURITY BREACHES

-
- *Global Network Operations Center 24x7 monitoring*

AT&T has a multi-tiered approach to detect and protect against security breaches within the network, databases and operational support systems.

AT&T's approach to developing methods to prevent, detect and report security breaches of [redacted] focuses on two distinct areas of the comprehensive end-to-end AT&T Security process:

[redacted]

[redacted] AT&T Labs [redacted]

[redacted] AT&T's [redacted]

[redacted] AT&T [redacted]

[redacted] AT&T's [redacted]

[redacted] AT&T's [redacted]

In directly linking a research staff engaged with exploring emerging security threats to an engineering / operations organization responsible for AT&T's worldwide security management, AT&T proactively adapts to new network threats. This continuous process of research, development, fielding and monitoring of traffic across AT&T's networks has resulted in tools that

leverage AT&T security analysts' abilities to safeguard network traffic and protect internal systems.

[redacted]

The contractor shall take all prudent measures to detect and prevent security breaches of the Networx program. [C.3.3.2.2.6]

Many of AT&T's Security Services for detecting and preventing security breaches are heralded as the industry's best. Products such as Internet Protect, Intrusion Detection Service, Managed Firewall Service and others are examples of AT&T's industry leading capabilities in network security.

In accordance with FISMA and OMB Circular A-130 Appendix III, an incident response capability will be provided for systems contracted under the Networx program to respond to and manage security breaches. A computer security incident is an adverse event in a computer system or network caused by a failure of a security mechanism or an attempted or threatened breach of these mechanisms. Section 4.9 of the Security Plan provides additional detail for AT&T's incident response capabilities. Furthermore, AT&T takes a proactive approach to preventing and detecting security breaches of its networks, [redacted], and databases by protecting [redacted]

[redacted] This capability of protecting AT”&T’s own infrastructure was previously described in Section 2.3.3.3, Information Security.

The contractor shall identify all security-related system and network vulnerabilities and take corrective measures to eliminate them, and upon request, advise Agencies how to best deter security breaches when using the contractor's Networx services. [C.3.3.2.2.6]

INCIDENT RESPONSE PLAN OUTLINE

- *Requirements for incident response handling*
- *Objectives for incident response handling*
- *Organizational structure for incident response handling*
- *Roles and responsibilities for key elements and personnel*
- *Preparation and training guidelines*
- *Policy and procedures for handling incidents*
- *Incident reporting procedures*

In accordance with FISMA and OMB Circular A-130 Appendix III, an incident response capability will be provided for systems contracted under the Networx program to respond to and manage security breaches. As detailed in section 4.9 of the Security Plan,, AT&T provides an Incident Response Plan, describing in detail the incident response procedures to be implemented in the event a security breach occurs.

[redacted]

Controls are implemented as appropriate to identify and correct security-related system and network vulnerabilities. With information obtained by observing and monitoring these controls, AT&T works with and advises the Government regarding efforts to deter security breaches and will advise agencies how to best deter security breaches when using our Networx services. AT&T will advise Agencies on best practice security awareness and preventive procedures for each service. This advice is offered in several methods, including security instructions included with the service operations documentation, Internet-based security awareness information and Best Practice information brochures.

The contractor shall report on the results of the investigation and the corrective measures applied to the security breach or problem within 4 hours of notifying the PMO and Agencies that a security breach, violation, or problem has occurred. [C.3.3.2.2.6]

The Networx Security Manager is responsible for reporting on the results of investigations and the corrective measures applied to identified security breaches and issues. These reports are submitted to the PMO and affected Agencies within 4 hours of their first notification a breach has occurred.

2.3.3.6 Alarms and Audit Trails [C.3.3.2.2.7]

The contractor shall provide and maintain real-time operational procedures and capability for detecting and monitoring suspected abuse or intrusions to the network and set off alarms for those events that require immediate attention by PMO, affected Agency or site, and/or contractor staff. [C.3.3.2.2.7]

The Government benefits from tested and proven security mechanisms that detect and respond to security-related events. AT&T will evaluate events and notify the GSA and affected Agency of any service-affecting security breaches or violations as required. AT&T is responsible for resolving security breaches relevant to Networx services and appropriately reports incidents to investigative authorities. Full cooperation is provided to all investigations. Also provided, upon request, are records, logs, or other evidence relevant to an investigation. When appropriate, [redacted] AT&T as required by the Government.

The Global Network Operations Center (GNOC) is responsible for the overall network management (surveillance, communication and support) of switched and data networks. The GNOC (**Figure 2.3.3.6-1**) owns, maintains, and executes the [redacted]

Figure 2.3.3.6-1: AT&T Global Network Operations Center Security Command. *The GNOC is a vital component of AT&T's measures to guard against intrusion or loss of government data.*

[redacted] The GSA and Agencies [redacted]

The GNOC serves as the Security [redacted]

[redacted]

The contractor shall maintain all information associated with security violations including the associated reports and alarm information from alarms logs associated with the violation for three years from the date of the incident, or of the report, whichever is later. [C.3.3.2.2.7]

The contractor shall make available all information associated with security violations including the associated reports and alarm information from alarm logs associated with the violation for three years from the date of the incident, or of the report, whichever is later. [C.3.3.2.2.7]

AT&T will maintain all information associated with any Networx security violations for three years from the date of the incident or report, whichever is later. This documentation includes the associated reports and alarm information from the alarm logs associated with the violation. The documentation will be made available to the Government upon request.

2.3.3.7 Physical Security [C.3.3.2.2.9]

The contractor shall physically protect and prevent unauthorized access to Networx services operations facilities, equipment, material and documents, and any other Networx related contractor facility and equipment that stores or handles Networx related information or data. [C.3.3.2.2.9]

Within the United States, network nodes are located in Central Office facilities, which are generally owned by AT&T. Some network facilities are located in buildings that may be owned by the incumbent Regional Bell Operating Company (RBOC). These facilities are large, disaster-resistant buildings, without windows, designed specifically to house telecommunications equipment. Access to these facilities is strictly controlled.

Because of AT&T's extensive experience with classified Government contracts, a culture of information security has developed and is instilled in the support staff. AT&T therefore, makes use of a multi-tiered approach to

effect protection of its facilities, using several key and powerfully proven methods as outlined in **Table 2.3.3.7-1**.

MULTI-TIERED APPROACH TO SECURING NETWORX FACILITIES

MULTI-TIERED APPROACH TO SECURING NETWORX FACILITIES
[redacted]

Table 2.3.3.7-1: AT&T's Multi-tiered Approach to Securing Networx Facilities. *AT&T's facilities are protected by various methods to prevent any means of physical breach.*

The contractor shall control access to its Networx services related facilities, equipment, material and documents by employees and visitors via electronic and/or physical methods corresponding to the critical nature of the work being performed, or the sensitive nature of the Government information being handled. [C.3.3.2.2.9]

AT&T utilizes various methods, both electronic and physical; to control access to its services-related facilities. [redacted]

Table 2.3.3.7-1. [redacted]

[redacted]

AT&T [redacted]

The contractor shall protect its Networx services operations facilities from basic service interruptions such as those caused by electrical outages, flooding, etc. [C.3.3.2.2.9]

All systems are monitored and have precise mechanisms and procedures to cope with basic service interruptions such as those caused by electrical outages, flooding, fire, etc.

Stringent practices are in place to protect facilities during normal operations or other situations such as construction. [redacted]

AT&T [redacted]

[redacted] Onsite building technicians, janitorial services, and/or service partners handle water leaks or water penetration.

[redacted]

[redacted]

AT&T's [redacted]

The contractor shall protect its Networx services operations facilities by meeting fire code regulations specific to the location of the facility. [C.3.3.2.2.9]

All locations currently meet or exceed local, state, and Federal fire code regulations. These high standards typically maintained through [redacted] compliant with OSHA requirements are in place to help ensure personnel are safely evacuated in the event of an emergency. Facilities are equipped with alarm and automatic fire prevention systems as required by the functions and equipment located at the facility. [redacted]

The contractor shall ensure offsite backup and storage of critical Networx services configuration and OSS data and information generated and stored at its Networx facilities. [C.3.3.2.2.9]

Backup and storage of critical customer data and information is currently provided to many Federal customers. AT&T does [redacted] offers a powerful combination, benefiting the Government with an outstanding level of redundancy assurance, and protection of information.

The contractor shall protect its Networx services hardware and software from theft or other human threats that may impact the availability of Networx services or compromise Government information or data. [C.3.3.2.2.9]

Each facility is protected from entry by unauthorized persons. Operations are conducted in highly secured environments where physical access to

switching centers, global network and service management centers, and other network facilities is strictly monitored and managed. Many strategies are employed to safeguard these assets, including:

[redacted]

AT&T facilities [redacted]

[redacted]

AT&T continues to use a multi-tiered approach combining the above with such measures as:

[redacted]

[redacted]AT&T[redacted]

[redacted]

2.3.3.8 Non-Domestic Services [C.3.3.2.2.12]

The contractor shall provide the best commercial security practices in supporting service delivery to non-domestic locations. **[C.3.3.2.2.12]**

AT&T has offered world-wide voice and data services for many years gaining valuable experience in service delivery and security challenges. For Networx, AT&T will provide our industry leading commercial security practices in supporting service delivery to non-domestic locations. As with any service that AT&T has partnered to provide a complete solution, all service and support data is closely monitored for its accuracy and integrity.

Outside the United States, network nodes are [redacted] AT&T's [redacted] (**Table 2.3.3.8-1**).

Methods for Securing Non-Domestic Network Nodes

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 2.3.3.8-1: Securing Non-Domestic Network Nodes. *Stringent security methods to protect network nodes are employed internationally.*

2.3.3.9 Ongoing Security Refreshment [C.3.3.2.2.11]

The contractor shall be proactive in improving the security of Networx services, databases, and OSS, and shall describe in the Security Plan the contractor's approach for keeping appraised of the latest threats, modernizing with the latest trends, methods, and technologies for preventing and detecting security breaches, and improving overall Networx security throughout the life of the contract. [C.3.3.2.2.11]

AT&T uses several methods, techniques and technologies to keep informed of the latest threats to security breaches. These are used to prevent and detect security breaches and to maintain and improve Networx security over the life of the contract.

A Security Risk Assessment [redacted] As part of this assessment, [redacted] AT&T [redacted] Government [redacted] Networx services, [redacted]

AT&T will [redacted] AT&T [redacted]

Another method for security refreshment is the re-evaluation and continuous improvement accomplished within AT&T through a combination of expert councils and trend analysis. The AT&T Security [redacted] AT&T's major security programs and core functions. One of the primary goals [redacted]

AT&T also gains insight into emerging trends or threats through active participation in global and industry security organizations such as CERT/CC (Computer Emergency Response Team Coordination Center), FIRST (Forum of Incident Response and Security Teams), IETF (Internet Engineering Task Force), W3C (World Wide Web Consortium), NSTAC (National Security Telecommunications Advisory Committee), NSIE (National Safety Information Exchange), and many others.

AT&T actively participates in employee education and training programs, where most security professionals hold the Certified Information System Security Professional (CISSP) credential. Employees also hold Certified Information Security Auditor (CISA), Certified Cisco Internet Engineer (CCIE), Information System Security manager (ISSM), Certified Wireless Network Administrator (CWNA), and other industry certifications. To keep the certifications current, the employees must participate in training programs by taking classes either on-line or in-person.

AT&T uses a combination of commercial and proprietary information security applications to maintain and secure Networx services, Networx [redacted]

[redacted] AT&T will [redacted] AT&T will [redacted]

[redacted] AT&T also maintains close relationships with the major hardware and software vendors in order to be kept informed of new exploits prior to general broadcast to the public. Having first hand knowledge gives AT&T time to prepare mitigation strategies. AT&T participates in vendor forums and workshops and keeps personnel fully trained and informed of security issues by subscribing to the major alert bulletin e-mail distribution lists.

The continual reassessment and improvement of security policies as described above will be used to improve overall Networx security throughout the life of the Networx contract.

The contractor shall be proactive in ensuring the effectiveness of its management, technical, and operational security controls, and shall describe in the Security Plan how it plans to ensure the effectiveness of security controls throughout the life of the contract. [C.3.3.2.2.11]

Several key methods are used to maintain the effectiveness of management, a key component of the overall Risk Management program. AT&T views Risk Assessment as an on-going part of security risk management covering the periods of pre-award, award, and post-award. The risk management programs looks at all phases of the overall program to include both personnel and systems issues.

Sections 3,4, and 6 of the AT&T Security Plan (Appendix C) further and more specifically addresses the effectiveness of its management, technical, and operational security controls, and describes plans that maximize the effectiveness of the security controls throughout the life of the contract.

The contractor shall be proactive in ensuring that security is considered as part of any new deployments or changes to services and OSS, and shall describe in the Security Plan how it will ensure that security is considered and built into new Networx services deployments and enhancements, new OSS deployments and enhancements, and Networx services and OSS configuration changes. [C.3.3.2.2.11]

The life cycle approach will be applied initially, as well as to all future enhancements, new deployments, and configuration changes for systems,

networks, and services contracted for under Networx. To protect the confidentiality, integrity and availability, as defined in FIPS publication 199, of Government information, databases, Operational Support Systems (OSS), and information systems, and to provide fundamental uniformity as the

Government transitions to commercially managed IT solutions, [redacted] NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*.

Prior to any new deployments, changes to services and OSS, and any enhancements, AT&T will take security into consideration and it will be evaluated by the Change Control Board. AT&T will support any Networx system security [redacted]

The Contractor shall ensure throughout the life of the contract that all Networx OSS and service components software have current and up-to-date security updates and patches for all known vulnerabilities. [C.3.3.2.2.11]

AT&T has held various Government contracts and, during the management of these contracts, has continued to maintain the OSS and other service components software to current and up to date standards with regard to security updates and patches for all known vulnerabilities. [redacted] AT&T [redacted] These controls are [redacted]

These controls [redacted] Networx Security Plan (Appendix C). AT&T employs the [redacted] AT&T internally

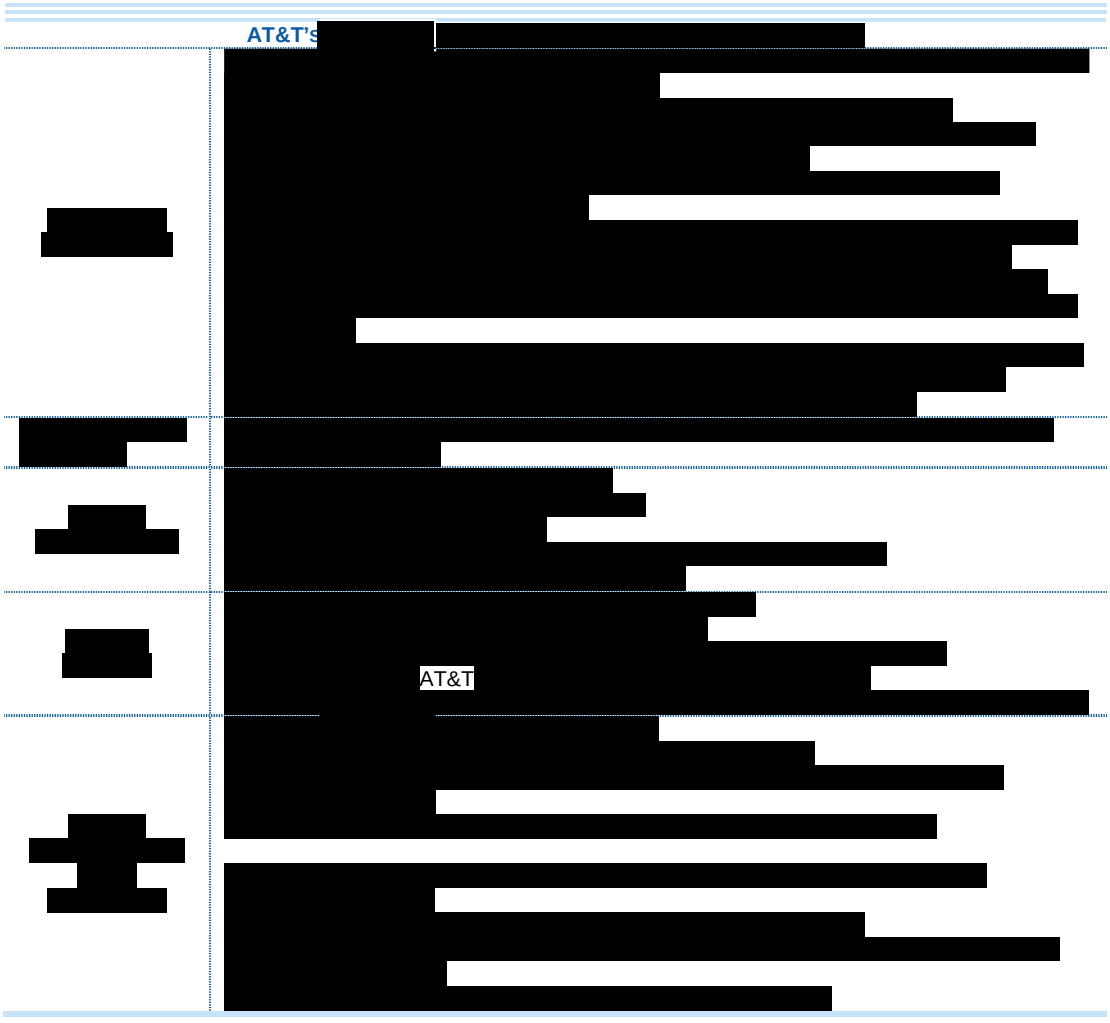
developed [redacted]

2.3.3.10 Fraud Prevention Management [C.3.3.2.2.13]

The contractor shall take a proactive approach in developing methods to prevent, detect and report fraudulent use of services and the contractor shall describe in its Security Plan the approach for modernizing with the latest fraud prevention and detection trends, methods, and technologies and for improving fraud detection and prevention capabilities throughout the life of the contract. [C.3.3.2.2.13]

As stated previously in section 2.3.3.2, Security Management Capabilities, [redacted] is responsible for minimizing or averting losses through on-line, near real-time detection of fraud alerts for the GSA and subscribing Agencies. The Government's data is continuously and automatically analyzed as [redacted] database is mechanically reviewed for fraudulent usage patterns.

AT&T's [redacted] **Table 2.3.3.10-1**.



AT&T's [redacted]
[redacted]

Table 2.3.3.10-1: AT&T IP Network Fraud and Abuse Center Responsibilities. [redacted]

Section 6.15 Fraud Prevention Management of AT&T's Security Plan, Appendix C, describes our approach for modernizing with the latest fraud prevention and detection trends, methods, and technologies and for improving fraud detection and prevention capabilities throughout the life of the contract.

Proactive Approach to Fraud Protection for Networx Wireless Services

The Government benefits from a multi-tiered fraud detection and prevention program **(Table 2.3.3.10-2)** as included with the wireless services provided by Cingular Wireless through AT&T's Networx program.

CINGULAR'S METHODS FOR PROTECTION FROM FRAUD AND ABUSE	
[redacted]	[redacted] Cingular Wireless [redacted]
[redacted]	[redacted]
[redacted]	[redacted]
Cingular Wireless [redacted]	[redacted] Cingular Wireless [redacted]

Table 2.3.3.10-2: Cingular's Fraud and Abuse Protection Program. *This comprehensive approach to fraud detection and analysis provides the Government wireless service without concern of fraudulent usage.*

Technological advances in the Cellular Personal Communications industry have virtually eliminated “cloning” fraud from occurring. Today, two types of fraud are monitored and reported with wireless services from AT&T as well as throughout the industry, Subscription Fraud and Equipment Fraud.

Subscription Fraud is defined as an account or line of service that was opened without the authorization of the Company or person whose name and information is on the account. Once identified, these accounts are cancelled immediately. Typically there are equipment, usage, and/or monthly recurring charges uncollected on these accounts.

Equipment Fraud is defined as a legitimate account that had unauthorized equipment ordered shipped and charged on the account.

The monthly Networx Fraud Performance Measurements Report will include:

- Number of incidents of Subscription and /or Equipment Fraud
- Total dollar amount incurred from the reported Networx Wireless fraud incidents in the reporting period
- Number of requests from Agencies for information concerning investigations of abuse of the services in the reporting period
- Status of AT&T’s investigations of fraudulent use of services, including number of investigations opened during the period, closed during period, active at end of period, and inactive at end of period.

The contractor shall take all adequate and prudent measures to detect and prevent fraud abuse related to the Networx program. [C.3.3.2.2.13]

The Government can be confident that AT&T’s fraud management capabilities throughout its service offerings will also be leveraged in support of the Networx services. These capabilities will be managed within the Contractor CPO with oversight by AT&T’s Networx Security manager.

AT&T's approach to fraud prevention is to implement and manage extensive security controls to prevent, detect, and report fraudulent use of services for the Networx program. AT&T has a comprehensive calling card fraud prevention system to handle millions of cards distributed globally on an annual basis. **Table 2.3.3.10-3** lists some examples of fraud controls employed by AT&T.

AT&T FRAUD PREVENTION CONTROLS
[redacted]
AT&T
[redacted]
AT&T
The AT&T
AT&T

Table 2.3.3.10-3: AT&T Fraud Prevention Controls. *The Government benefits from AT&T's* [redacted]

The contractor shall identify all fraud-related system and network vulnerabilities and take corrective measures to eliminate them, perform message and calling pattern analyses prior to and after billing, investigate annoyance calls, investigate incidents of programmed system and network computers programmed in error, and advise Agencies how to best employ fraud prevention and detection techniques when using the contractor's Networx services. [C.3.3.2.2.13]

AT&T's [redacted]

[redacted] AT&T performs [redacted] AT&T does perform and will provide [redacted] AT&T Government Solutions.

[redacted]

[redacted] AT&T will [redacted] Agencies [redacted] Networx services [redacted] Networx service [redacted] AT&T [redacted]

[redacted] and Best Practice brochures to advise Agencies how to best employ prevention and detection techniques when using our services.

Wireless Services Fraud Protection

Cingular Wireless has launched a multi-faceted, aggressive prevention campaign to combat wireless fraud, which includes implementation of the following measures:

[redacted]

[redacted]

If the Offeror's approach to meeting Security Management requirements is different for optional services than for mandatory services, the offeror shall describe the differences in a separate optional services sub-section within the Security Management section of the Offeror's response. The Offeror shall reflect differences due to optional services in an addendum to the Security Plan.

AT&T's approach [redacted]

2.3.3.11 Summary

The GSA and subscribing Agencies can be confident that their AT&T provided Networx services are protected from unauthorized access, disclosure, corruption, or disruption of service by the most advanced capabilities in the industry. Through the support of comprehensive and extensive security organizations, policies, and innovative processes and products, AT&T will deliver Networx services with industry leading and uncompromised security.

AT&T currently provides network services to most major banks and other financial institutions, as well as [redacted] Government customers. AT&T [redacted] guides are enforced through Security Evaluation Programs and other risk assessments and vulnerability scans as well as awareness training for employees, contractors and customers. These corporate polices meet [redacted] OMB, NIST and FIPS standards and guidelines, and the GSA and Customer Agencies can be confident that their AT&T provided Networx services are protected and supported to comply with FISMA requirements.

AT&T Labs is responsible for research and development of some of the most innovative and effective security products and processes used in the industry today. AT&T's leading position in the industry with regard to security and protection of information is maintained through the adoption of innovative products such as Internet Protect [redacted] In addition, AT&T participates in industry security organizations and forums to retain its industry-leading position. This cutting edge and industry leading support is what the Government can expect when securing services from AT&T Networx.

[redacted] Support in the Networx Contractor's Program Organization and Customer Support Office is available 24X7 [redacted] Security Plan (Appendix C) [redacted]

[redacted] AT&T's [redacted] AT&T's [redacted] For wireless fraud protection, a multi-tiered approach, including authentication, detection and analysis processes, virtually eliminates these security incidents for the Government.

As Agencies may require specific safeguards for the services being provided, they can be assured of effective security solutions customized to

their specific needs. FISMA, FIPS and NIST requirements can be met for Agency specific custom solutions.

The Government will receive Networx services that are secure and protected from unauthorized access, disclosure, or corruption by a comprehensive array of security processes, products, procedures, and professional support.

Table 2.3.3.11-1 [redacted] AT&T's [redacted]

FEATURES:	BENEFITS:
[redacted]	[redacted]
Global Network Operations Center	The Government's network services receive 24X7 global monitoring from the industry's best equipped operations centers.
AT&T Labs	The Government gets service support from one of the industry's most prolific communications and IT services research and development organizations.
[redacted]	Government [redacted]
AT&T [redacted]	Government [redacted]
AT&T [redacted]	[redacted] Government
Wireless Fraud Prevention Program	This multi-tiered solution to detect and prevent wireless fraud ensures the Government of secure and uninterrupted wireless service.
Comprehensive Security Plan	Provides the Government a complete guide to Security processes for Networx Systems or services provided.

Table 2.3.3.11-1: *Features and Benefits of AT&T Security Management Solutions.*