2.3.3   Security Management [L.34.2.3.3, C.3.3.2]

Security is one of the most important attributes of each service provided to the Federal government. Security and protection for AT&T services are also a key mandate within AT&T, as they are considered the cornerstone of AT&T's services and service delivery. This security policy emphasizes that customer data and communications will be safeguarded from unauthorized access, disclosure, corruption or disruption of service, and is applicable to all service elements, systems, applications and workstations used to support Networx services provided by AT&T.

2.3.3.1   Security Plan [L.34.2.3.3, C.3.3.2.2.1]

The offeror shall provide a Security Plan that addresses how the offeror proposes to meet Government Security Management requirements specified in Section C.3.3.2, Security Management. The offeror shall structure the Security Plan according to requirements specified in Section C.3.3.2.4.2.1, Security Plan and Risks Assessment.

The Security Plan (Appendix C) provides a blueprint for safeguarding all AT&T service elements, systems, applications and workstations from unauthorized access, disclosure, corruption or disruption. The plan that has been provided with this proposal details how the Government's Security Management requirements are to be met, and describes the initiatives, processes and procedures administered by AT&T's security organizations worldwide for application of necessary security controls for the Government's Networx services.

The Security Plan also addresses in detail the functional elements as outlined by the General Services Administration (GSA) and illustrated in **Figure 2.3.3.1-1**.

The plan is formatted to meet the National Institute of Standards and Technology's (NIST) SP 800-18 recommendations. An outline for Risk Assessment formatted as
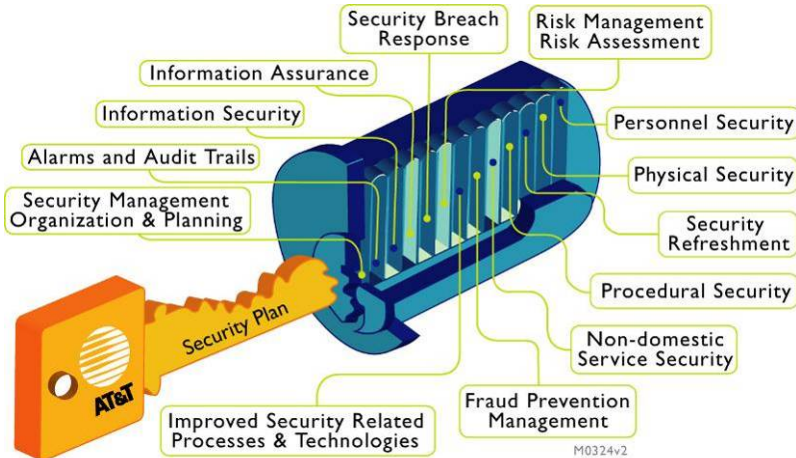
Figure 2.3.3.1-1: AT&T's Networx Security Plan. *AT&T's Networx Security Plan provides GSA and Agencies a clear understanding and reliable expectation regarding how Networx related security issues are to be managed.*

defined in the NIST SP 800-30 is attached to the Security Plan. AT&T also uses the following NIST special publications for reference and guidance in developing the Government's security plans:

The GSA will receive a Networx Security Plan at contract award (included with this proposal in Appendix C). A revised Security Plan, as well as a completed Risk Assessment for Networx services will be delivered within 30 days of the Notice to Proceed. The Security Plan is updated annually, or more frequently if security-significant system changes are made.

The offeror shall describe in the Security Plan its security management organization, resources, strategies, practices, policies, processes, procedures, tools, systems, reports and any other relevant capabilities to provide the

Government with a high degree of confidence that the offeror has sound, effective, and adequate security management controls, technical controls, and operational controls that meet Government security management requirements.

To meet critical Government security requirements, comprehensive security organizations are maintained at corporate and worldwide levels. These organizations are dedicated ███████████████████████████ AT&T global network, ████████████████████████ ███████████████████████████████████ ███████████████████████████████████ ███████████████████████████████████ ██████████████████████████These organizations are further detailed in Section 6, Supplemental Information, of the Security Plan (Appendix C).

Through these organizations, AT&T maintains a library of documents and guidelines that establish corporate security policies regarding all aspects of providing, maintaining, and managing AT&T delivered products and services including AT&T Networx provided services. AT&T's ████████████████ ███████████████ documents comprise this comprehensive security policy library and are described in more detail in the Security Plan Section 6.1, Security Management Organization.

The GSA and subscribing Agencies can be confident that AT&T's Security management within the Networx CPO will utilize these resources as needed in support of their Networx services. The Networx CPO Security management is available to support the GSA and subscribing Agencies around the clock.

The GSA and subscribing Agencies will benefit from AT&T's consistent approach and strategies to delivering secure Networx services. The most effective service security designs and implementations must be continuously managed and analyzed for improvement, as illustrated in **Figure 2.3.3.1-2**.

AT&T views service security as a process driven by management and user awareness and supported by expert skills and advanced technology. System security is a fundamental concept in all network components, from workstations, transport devices, servers, applications and access methods. More details are provided in Section 6 of the Security Plan.

Figure 2.3.3.1-2: AT&T's Continuous analysis process. *Continuous analysis of Government assets to apply best security practices.*

The Networx Security Plan is designed to protect the Government's and AT&T's services, information, resources, and systems from fraudulent usage, unauthorized access, or service disruption, including the protection of Networx services from other Government departments and Agencies. The detailed Security Plans will allow the GSA and subscribing Agencies to know how the Networx services are protected as well as what processes will be engaged in the event of a security issue.

The contractor's Security Plan shall describe in detail how the contractor shall satisfy the security requirements as identified in Sections C.3.3.2, Security Management, and all its subsections, including how improved security-related processes and technologies are to be incorporated into the contract as they become commercially available. See Section C.3.3.2.4.2.1, Security Plan and Risks Assessment for report requirements. **[C.3.3.2.2.1]**

As illustrated in **Figure 2.3.3.1-1**, the Security Plan (Appendix C) details how the Government's Security Management requirements are to be met. There are six major sections in the Security Plan. Sections 1-5 of the Security Plan follow the format suggested in NIST Special Publication 800-18.

SECURITY PLAN SECTIONS

- *System Identification*
- *Sensitivity of Information Handled*
- *Management Controls*
- *Operational Controls*
- *Technical Controls*
- *Supplemental Information*

 Section 6 of the Security Plan details the areas the GSA has specifically required in the Security Plan, including how improved security-related processes and technologies are to be incorporated into Networx as they become commercially available and implemented within AT&T's service delivery platforms.

The contractor's Security Plan shall include a description of the approach, scope, and methodology of Networx services security risk analyses that shall be undertaken by the contractor throughout the life of the contract. [C.3.3.2.2.1]

AT&T pays the highest attention to protecting its network resources and its customers' information and services. The level of security enables AT&T to deliver service that consistently meets or exceeds customers' expectations, as well as applicable regulatory and legal requirements.

As part of the activities and resources devoted to fostering network security, AT&T maintains a staff of several hundred professionals dedicated to network security. Extensive documented security policies govern the security of the network, systems, and applications within the AT&T worldwide network. The policies are complemented by operational processes and procedures, reviews, assessments and audits. AT&T uses a comprehensive set of company designed and off-the-shelf tools and technologies to detect, prevent, analyze and respond to security vulnerabilities and attacks. A detailed description of the approach, scope, and methodology of Networx services security risk analyses that AT&T performs throughout the life of the contract is found in Section 3.1 of the Security Plan (Appendix C), Risk Assessment and Management and Section 6.6, Security Risk Management.

The contractor's Security Plan shall comply with the requirements of Section C.2.1.11, Networx Security. [C.3.3.2.2.1]

Comprehensive AT&T ███████████████████████████████ contain industry leading standards for deploying network and physical security controls. AT&T currently supports

networks at ██

██

██

████████████████████████████████ Security engineers have expert knowledge of Government security requirements outlined in Office of Management and Budget (OMB) A-130, Federal Information Security Management Act (FISMA), and the NIST 800 series of Special Publications, as well as National Information Assurance Certification and Accreditation Process (NIACAP) and Defense Information Technology Security Certification and Accreditation Process (DITSCAP) methodologies and agency-specific requirements.

Many network solutions are granted Authority to Operate (ATO) as a result of the Certification and Accreditation (C&A) process executed by the AT&T security team. AT&T is well versed in the deployment of enhanced security mechanisms for data networks, such as multi-layered security applications ████████████████ encryptions as well as Federal Information Processing Standards (FIPS) compliant encryption mechanisms. More information regarding AT&T's approach to these requirements is further detailed throughout the Security Plan (Appendix C).

This extensive body of knowledge and capabilities meets or exceeds the requirements of the Standards and Guidelines indicated in section C.2.1.11 of the RFP, and is applicable to all service elements, systems, applications and workstations used to support AT&T provided Networx services.

The contractor shall describe in the Security Plan its Networx security management organization, and how it will interface and coordinate with suppliers, vendors, partners, and Government to address Networx security related matters. [C.3.3.2.2.1]

Networx security is managed in the CPO by the Networx Security Manager. ████ Networx Security Manager, ██████████████████████████████████ AT&T

██████ Networx services ███████████████████████████████

GSA's and Agencies' █████████████████████████████████████

Networx Security Plan (Appendix C). The Security Manager is ████████

██

████████████████████████████ to the GSA and appropriate Agencies.

The Networx Security manager has the support of all of AT&T's security organizations as described in this section. Within the Networx CPO, as illustrated in **Figure 2.3.3.1-3,** the Security Manager has support from other functional areas and the authority to acquire information from these support teams as required for specific investigations, tasks, or emergencies.

Exacting security requirements are required when establishing relationships with subcontractors and suppliers. Subcontractors and suppliers must adhere to fitting

Figure 2.3.3.1-3: The Security Manager within AT&T's CPO. *The* ████████████████████████ ████████████████████████

policies and requirements necessary to secure AT&T networks, systems, and the data stored or traveling through the infrastructure. ████████████████████ ██

AT&T's ████████████████████████ AT&T's ████████████

████████████████████████████████ AT&T's ████████████

within the CPO, ████████████████████████████████████ to maintain
the GSA's and subscribing Agencies' security requirements for delivering
Networx services. The Government can be confident that AT&T's integrated
products, services, and solutions will be delivered with defined and consistent
security processes established and managed from end-to-end.

The contractor shall describe in the Security Plan the management, technical and operational controls as defined in
NIST SP 800-18, that will be employed to ensure the integrity, confidentiality, and availability of Government
information and data that is transported and/or stored by Networx services, Networx OSS, databases, or handled
manually at contractor's facilities. [C.3.3.2.2.1]

The Networx Security Plan (Appendix C) details both Operational and
Technical controls employed to maintain proper security relevant to all AT&T
provided Networx services. **Table 2.3.3.1-1** identifies the operational and
technical controls, as defined in NIST SP 800-18 and detailed in the Networx
Security Plan.

Table 2.3.3.1-1: Operational and Technical Control Areas Addressed in the Networx Security Plan.
████████████████████████████████████ *NIST SP 800-18.*

The Operational and Technical controls are detailed in Sections 4 and 5 of
the Security Plan for all Networx services.

The contractor shall describe in the Security Plan how it will communicate and educate its employees, vendors, and
Government users its Networx security policies, practices, and procedures, and how it plans to develop and maintain
overall security awareness among Networx stakeholders. [C.3.3.2.2.1]

The Government will find established policies and processes for proper
education and continued awareness of current security for all Networx service
stakeholders defined in Section 4.8, Security Awareness and Education. The
awareness and education program focuses on Networx service usage and
procedures for reporting security incidents.

*Use or disclosure of data contained on this sheet
is subject to the restriction on the title page of this proposal*   **AT&T Proprietary**   **Page 111 of 493**
March 5, 2007

The Networx Security Manager is responsible for presenting security awareness information to everyone with system access, as well as providing relevant Security Plan information. The security awareness and education program is also designed to inform the user on how to get assistance when having difficulty using the system or reporting security incidents.

The Networx Security Manager also oversees these requirements are met for all subcontractor employees contracted to work on Networx provided services. The subcontractor training and professional development is documented and monitored. **Table 2.3.3.1-2** is a checklist of the security awareness training responsibilities of the Networx Security Manager.

SECURITY AWARENESS AND EDUCATION REQUIREMENTS CHECKLIST

Table 2.3.3.1-2: AT&T's Security Awareness and Education Requirements. *AT&T's* ▮▮▮▮ *Government* ▮▮▮▮ *Government* ▮▮▮▮

AT&T Government Solutions personnel are given initial Security Training and then must go through an annual refreshment course. ▮▮▮▮▮▮▮▮▮▮ ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮ AT&T Security Manager ▮▮▮▮▮▮▮▮▮▮▮▮▮▮ This Security Training will include Networx security policies, practices, and procedures.

Networx Security requirements are incorporated into our subcontracts with vendors. Vendors must adhere to the same guidelines and AT&T's policies, practices, and procedures are communicated to them. As part of our on-going relationship with our vendor, updates to Security practices are communicated as needed.

Security awareness is communicated to Government users ███████ ██The Networx subscriber web-site will include information about Networx security policies, practices, and procedures. Networx DAR and Operations training will include an optional module on Security awareness.

██ AT&T's ████████████████████████████
████████████ AT&T and the Government ████████████
████████████████████████ AT&T's ████████████████
██
██
██
███████████████████████

██
████████████████████████████████████non-AT&T
██
██
██Non-
AT&T ██
██████████████████████████

2.3.3.2   Security Management Capabilities [L.34.2.3.3]

The offeror shall describe its security management capabilities to provide the Government a high degree of confidence that the offeror will be a strong partner that understands the challenges that the Government faces in:
(a) Ensuring integrity, confidentiality, and availability of Government information given the wide range of Networx services, users, and geographical locations

2005 Winner

AT&T Internet Protect Honored with Stevie Award for Best New Product or Service in Telecommunications.

--The American Business Awards, 2005

World Communication Awards: 'Best Technology Foresight' for AT&T Internet Protect.

October 2004

Stratecast Partners

AT&T receives the "2005 Best-in-Class NSP Managed Security Services Award" for being "best positioned to serve the broadest and largest number of customers and create strategic differentiation for the company (either as AT&T or the merged AT&T and SBC) in the evolving communications industry."

April 2005

AT&T has a reputation as an industry leader in network security. The Government's Networx services, information, and information-processing resources are protected against threats, attacks, or failures of systems in accordance with these industry leading practices and technology. AT&T relies ██

██ **Table 2.3.3.2-1**.

	SECURITY CONTROLS AND PROCEDURES
Network	████████████████████████████████████
	████████████████████████████████
	████████████████████████████████████
	████████████
Operations Support Systems	██
	██
Physical Facilities	████████████████████████████
	██████████████
	████████████████
	██████████████████
	████████████
Personnel	████████████████████████████████████
	██████████████████
	██████████████████

Table 2.3.3.2-1: AT&T's Security Controls and Procedures. ████ *Government's* ████████████
████████████████████████

These controls, in conjunction with risk analysis and a set of detailed security services, maintain the security of AT&T's offered services and service delivery infrastructure. The Security Plan (Appendix C) details the specific risk

management processes and controls for securing these Government services, as required by the GSA and Customer Agency.

(b) Meeting the security needs of a large and heterogeneous geographically distributed user community

AT&T is truly a global company that reaches around the world with a company-owned network backbone. The Government can be confident that AT&T's stringent security policies are consistently followed throughout the reach of its network. With ▉ Federal Government customers and ▉ ▉ of the S&P 500 companies as customers domestically and around the world, AT&T is prepared for most any required solution customized or standard to meet the Government's specific needs.

The Security Plan implemented by AT&T (Appendix C) is designed to reduce vulnerabilities, adapt to new threats, and help ensure that Networx security management capabilities are maintained to the latest standards and practices. The life cycle approach, as defined in NIST 800-14, is embedded into the Security Plan and will be applied to all future enhancements, new deployments and configuration changes for systems, networks and services contracted under Networx.

Use or disclosure of data contained on this sheet
is subject to the restriction on the title page of this proposal
AT&T Proprietary
Page 115 of 493
March 5, 2007

██████████████

███████ Government

Agencies, AT&T██████████

███████████

████████████

████████████

████████████

███████████

██████████**Figure 2.3.3.2-1**)

████████████

███████████

███████████

█████████

████████████

███████████

████████████

████████████

████████

████████████

Figure 2.3.3.2-1: AT&T Provides Various Custom Solutions.
████████████████████████

███████████

████████████████████████████

███████████████████████████

(c) Preventing and minimizing waste, fraud, and abuse, and if applicable, prosecuting the perpetrators

The Government ███████████████████ AT&T's ██████████

████████████████████████████

████████████████████████████

████████████████████████████

████████████████████████████

██████████ ██

███

███

███

███████████████ records the fraud tracking efforts of AT&T's fraud analysts. In this way, ██████ can automatically monitor the Government's Networx call details for ████████████████████████████████████ ████████

AT&T's ██ is one of the world's largest databases, used for storing ███████████████ ████████████████████ AT&T ██████████████████████████ ███ ██ ████████

AT&T's security organization actively responds to subpoenas and assists various law enforcement agencies in capturing and prosecuting criminals suspected of committing telecommunications abuse and fraud. ████████ ███ ██████████████████████████████████████ AT&T ██ ███ ██████████ AT&T ██████████████████████████████ ██████████████████████████████████████ ██████████████████████████████████████ █████████████████████████████████ AT&T's ████████████ ████████████████████████████████████ ██

(d) Complying with security requirements and Executive Orders and keeping its security program updated with evolving Government standards and directives

The Government has an extensive history with AT&T customized systems including some of the most stringent and uniquely detailed security requirements designed for service delivery. AT&T Labs and the solution development engineers work together to provide innovative service solutions created to meet the Government's specific security requirements. The ability to maintain and update the security policy to the Government's evolving requirements is built into each and every solution. Some examples of unique and highly secure solutions are listed in **Table 2.3.3.2-2**.

AT&T CUSTOM GOVERNMENT SECURITY SERVICE SOLUTIONS

Table 2.3.3.2-2: AT&T Custom Government Security Service Solutions. *AT&T has designed many diverse secured communications solutions meeting unique and specific Government requirements.*

The Government can be confident of efforts to incorporate new or updated security standards and directives in the Networx service offerings and existing Agency solutions. AT&T maintains a leadership role in providing secure network services and participates in many Government and quasi-government organizations in the United States. By participating in these

*Use or disclosure of data contained on this sheet
is subject to the restriction on the title page of this proposal*   **AT&T Proprietary**   **Page 118 of 493**
March 5, 2007

organizations, AT&T is able to influence and track industry trends, capabilities and newer or evolving Government requirements.

AT&T PARTICIPATES WITH GOVERNMENT SECURITY ORGANIZATIONS

(e) Protecting Government operations and ensuring continuity of Government services.

The Government will benefit from one of the industry's most rigorous and thorough approaches to contingency planning and disaster recovery with AT&T's National Disaster Recovery organization. For years AT&T has continuously planned for undisrupted network operations during such natural disasters as hurricanes and floods. (For more detailed information on AT&T's Disaster Recovery capabilities, see section 2.3.4 of this proposal.) In addition to these planning efforts, within the United States, AT&T has cooperated with the Federal Government's National Special Security Events (NSSE) process since its creation in 1998, developing a disciplined contingency plan for each event that is NSSE designated.

Events are classified as NSSE based on a combination of factors,

The Government will receive a multi-phased approach to contingency planning for NSSEs as well as other significant events. The experience and skills of the NDR team in restoring AT&T services in the event of a disaster is

utilized for a detailed and thorough contingency planning process.

Table 2.3.3.2-3 ████████████████████████████████████ AT&T ██████████

██

	NATIONAL SPECIAL SECURITY EVENT / DISASTER RECOVERY PREPARATORY STEPS
1	███ ███████████████████ Global Network Operations Center (GNOC) ███████████████████████
2	███ ██████████████████████
3	███████████████████████████████ █████████████████████
4	███████████████████████████████████████
5	AT&T's Network Disaster Recovery team is put on alert ██████████████████ ██████████████
6	███████████████████████████████████
7	████████████████████████████████

Table 2.3.3.2-3: AT&T's NDR Preparatory Steps in NSSE Planning. *Strategic and thoughtful planning is essential to ensuring service availability for National Security events as well as Disaster Recovery.*

(f) Ensuring National Security

The GSA and subscribing Agencies benefit from AT&T's decades of experience working with Government Agencies and commercial enterprises on information security planning, implementation, and management. AT&T provides a wide range of security engineering and professional services to federal civilian and defense Government agencies, as well as State Government organizations providing National Security. AT&T's architects and engineers provide security solutions that:

██

    ███████████

██

    AT&T's ███████████████████████████████████

The Government has experienced AT&T's expertise in providing high profile security solutions, including:

- Seventy years experience in supporting classified and non-classified government projects

(g) Reducing vulnerabilities, adapting to new threats, and ensuring that Networx security management capabilities are maintained to latest standards and practices

A proactive approach is maintained to improve the overall security of any system contracted by the Government under the Networx contract throughout the system development life cycle. The Security Plan (Appendix C), Section 3.4 Planning for Security in the Life Cycle, provides details on the ▮▮▮▮▮▮(**Table 2.3.3.2-4**) ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮

PHASE	DESCRIPTION

Table 2.3.3.2-4: Five Phases of System Life Cycle. *Security is a priority through all phases of a system life cycle.*

In accordance with NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, each phase of the system development life cycle is included in the risk assessment in order to identify new threats and vulnerabilities and to implement mitigation controls as countermeasures. Additionally, there is flexibility in security planning in each phase to allow security requirements to be updated in response to new

threats and vulnerabilities identified as new technologies evolve and are implemented as part of an on-going and proactive security program.

The effectiveness of security controls is reviewed and assessed in each phase of the life cycle on a recurring basis as agreed by the GSA and Customer Agency. AT&T ███████████████████████████████████████ ███████Government ██████████████████████████████████████ █████████████████████████████████████The Security Plan is updated ████████████████████████████if security-significant system changes are made. Once the system is implemented, a risk assessment is performed annually in accordance with NIST 800-26, and the Risk Assessment is updated accordingly.

(h) Minimizing the impact of Networx related security breaches and attacks, and if applicable, prosecuting the perpetrators

AT&T has long been involved in computer and network security. Prior to the development of the Internet, AT&T has fostered an extensive security practice with the U. S. Government. The AT&T Labs Research organization has been involved with the Internet and its precursor since the late 1980s and has made contributions to many widely used strategic technologies, such as firewalls and Internet Protocol Security (IPsec).

AT&T Labs researchers have actively participated in the development of many facets of security technology through the Internet Engineering Task Force (IETF) and the Association for Computer Machinery's Special Interest Group on Data Communications (ACM-SIGCOMM) as well as serving the Internet Corporation for Assigned Names and Numbers (ICANN) and participating in security-related study committees as part of the Network Reliability and Interoperability Council (NRIC). Deep commitment to rigorous security discipline embedded throughout all processes, from desktop management to network and services is an extensive benefit for the Government.

Security expertise exemplifies the due diligence and discipline a service provider takes to successfully protect the network and computing infrastructures of the customers. AT&T's expertise was demonstrated by its ability to ward off the ██for millions of users on hundreds of ██ ██ ████████████████████████████ AT&T's ██████████████████████

AT&T adheres to the core security principles, illustrated in **Figure 2.3.3.2-2**, to address the key vulnerabilities.

Figure 2.3.3.2-2: Defense Strategies of IP Networks. ████████████████████████ *AT&T's* ████████ ████████

Security consultants stay abreast of current issues through participation in news groups and security forums as well as continuous education and actual resolution of client security issues. This breadth of expertise is a direct benefit to the Government in protection of Government services.

██

██████████████████████████████████████ AT&T's ██████████

██████████████████████████

Network security incidents include incidents such as, intrusions (e.g. attempted hacking, cracking, or other unauthorized access), denial of service attacks, spam attacks, and viruses or worms. ████████████ ██ is responsible for performing investigative techniques to ascertain the severity and motive behind network abuse ██ ███████████████████████████ After thorough investigation and review to determine customer involvement, appropriate actions are taken. If it is determined that a user is involved in a breach, warnings are issued and/or suspensions are recommended and implemented as agreed by the Government. When local or federal laws are broken, AT&T proactively engages law enforcement and fully supports investigation and prosecution activity. Quick action on these events further enforces and protects the Government's Networx services.

2.3.3.3 Information Security [C.3.3.2.2.4]

The contractor shall ensure confidentiality of data. [C.3.3.2.2.4]

The confidentiality, as defined in FIPS publication 199, of the Government's data is protected within the infrastructure through operational and technical controls as outlined in section 2.3.3.1 and as detailed in the Security Plan (Appendix C). These controls are in place to allow access to data only by those stakeholders authorized to access it.

Protecting the Government's information within a network infrastructure, regardless of the medium in which it resides, is an integral part of each business plan, system design, system/application implementation, and associated operation. ███████████████████████████████████████ ███████████████████████████████████████ ███████████████████████████████████ ████████ are techniques employed to safeguard Government's data.

Privacy of customer communications is fundamental. The commitment to safeguard privacy of customer communications takes on added significance as the global network for voice, data, and multimedia transmissions expands and becomes more interactive and accessible.

CUSTOMER PRIVACY

AT&T ████████████████

AT&T's ██████████

████████████████████████

████████████████████████

████████████████████████

███████████████████████

████████████████████

██████████████████████

███████ AT&T ████████████

██████████████████

█████████████████████████████████████ AT&T's ██████████

██

███████████████ Government's ████████████████

Wireless Service

Wireless services provided by Cingular use encryption as an important security mechanism to protect both user data and network control information.

██

██

████████████████████████████████████

████████████████████████████████████

████████████████████████████████████

███████████████████████████████

████████████████████████████

████████████████████████████████████

██████████████████████████

████████████████████████████████████

███████████████████████████████████

██████████████████████████

███████

Encryption protects information about user identities. Prior to encryption, the network protects user identities by minimizing transmission of user identity information, and by using temporary identifiers.

██

██████████████████████████████████

██

████████████████████████████████

███████

The contractor shall follow Federal Government-accepted security principles and practices per NIST SP 800-14, or better, to protect Government information in the contractor's infrastructure from disclosure to unauthorized persons. [C.3.3.2.2.4]

Security is an imperative and integral part of AT&T's services delivered worldwide, and this corporate mandate also commits to protecting Networx information and resources from unauthorized access, disclosure, corruption or disruption of service. The security organizations within corporate and

worldwide operational units incorporate the recommended NIST SP 800-14 principles and practices to develop and maintain these policies as appropriate.

The security practices protecting Government information in AT&T's

███

AT&T's ██ **Table 2.3.3.3-1**, ██

███

██████████████████████

KEY NIST SP 800-14 PRACTICES FOR PROTECTION OF INFORMATION	KEY AT&T PRACTICES FOR PROTECTION OF INFORMATION	
██████████████████ ██████████████	AT&T ████ ████ █	████████████████████ ██████████
		████████████
██████████████ ████████████	███████████████████ ████████████████	
████████████ █████████████████	███████████████████████ ███████████████████████ ██████████████████	
██████████████ ████████████████	AT&T ████████████████ ████████████████ ████████████	
████████████████		

Table 2.3.3.3-1: AT&T Security Practices vs. NIST SP 800-14. *The NIST SP 800-14* ████████████████████ █████████████████████████████████

Security compliance is central to AT&T's culture and is a condition for employment. Each management and staff employee is aware of this responsibility and is required to comply on an ongoing basis. AT&T's Security Center of Excellence and Corporate Security organizations manage and maintain corporate responsibility for enforcing these policies. The Security Manager, located in the CPO, manages these requirements for AT&T provided Networx services.

The contractor shall ensure data integrity. [C.3.3.2.2.4]

System and process design and development, as well as virus and intrusion protection, are primary areas of focus for protecting the Government's data. Designing and developing the operational support systems infrastructure and automated processes with the priority of protecting customer data from vulnerabilities is an essential mandate for AT&T and maximizes data integrity.

AT&T emphasizes the protection of the support systems from viruses, worms and other disruptive influences to maintain data integrity and availability. In support of this effort, AT&T takes the following steps with individual and corporate access equipment to ████ or service providing systems:

██

████████████████████████ AT&T ██

██

████████████████████

██

████████████████

██████████████████████████████████

██

████████████████

██

████████████████████████

██████ Company authorized ████████████████████████

████████████████████████████████████Company

████████████████████Company████████████████████

██

██████Company██████

Under the development leadership of AT&T Labs, the operational support systems are being driven to a Concept of One ███ ████████████ The Concept of One, highlighted in **Figure 2.3.3.3-1,** essentially directs that each of the services' support systems, such as billing, inventory, fault

InfoWorld

Hossein Eslambolchi was named one of "the 25 most influential" CTOs in InfoWorld's 2005 Top CTO Award, for his pioneering "Concept of One and Concept of Zero" philosophy.

–April 2005

management, and provisioning be converged over time until one common set of systems will handle multiple network, operations and service domains. This concept enables consistency and coordination in service delivery for all Networx services while improving data integrity with the enterprise-wide database architecture. Consequently, the Government gains more reliable service with fewer errors.
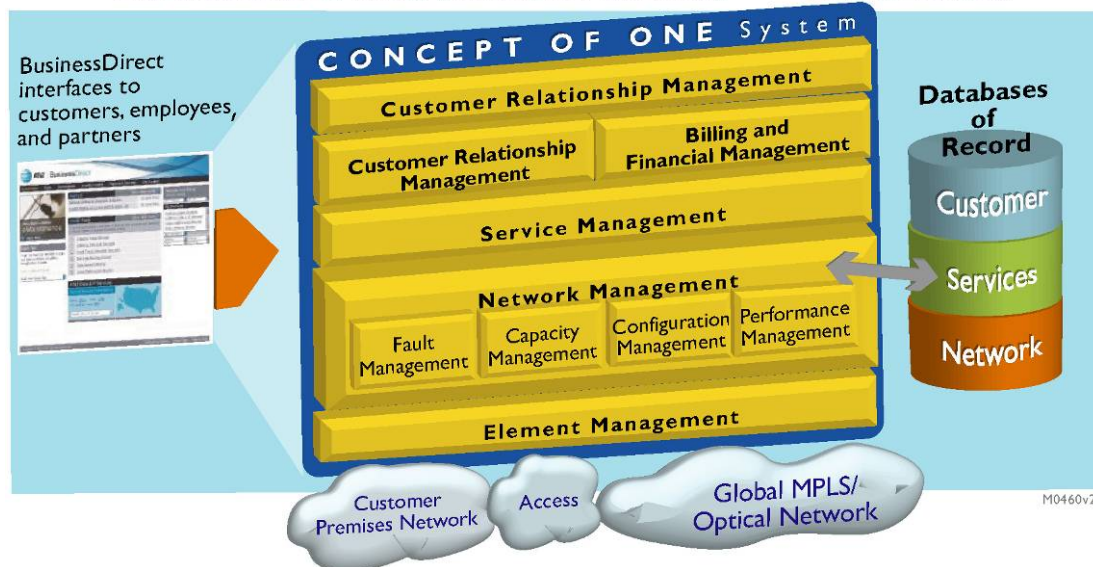

Figure 2.3.3.3-1: AT&T's "Concept of One" Approach to Support Systems Development. *More streamlined support system development equates to improved data integrity.*

Figure 2.3.3.3-2)

███

███

███████████████████████████████████████ AT&T's

███████████████████████████████████████

███

████████████████████████████

Figure 2.3.3-2: Concept of ████. █████████ *AT&T's* ████████████████
████████████████

AT&T's MPLS Network exemplifies these concepts by converging services within a single network and helping to ensure data integrity with how traffic is separated as well as the use of automated perimeter security devices. The MPLS standard is specifically designed to prevent unauthorized disclosure or modification of Virtual Private Network traffic by other users of the MPLS Network. Seamless integration and automation has been employed to manage and protect the traffic within the network.

The contractor shall protect the Government information from unauthorized modification while contained within the contractor's infrastructure. [C.3.3.2.2.4]

Integrity controls protect the system and the data processed, stored, and/or transmitted from accidental or malicious alteration or destruction. Integrity

controls also provide assurance to the Government that the information meets quality requirements and has not been altered. Validation controls are tests used to determine compliance with security specifications and requirements. ████████████████████████████████████

████████████████████████████████████

████████████

████████████████████

████████████████████████████

████████████████████████████

██

████████████████████████████

Message Integrity

██

██

██

████████████████

Use of Mobile Code

██

██

██

██

██

████████████████

██

████████████████████████████████████

████████████████████

██

██

███████████████

The contractor shall ensure identification and authentication of personnel involved in the operation and management of Networx services. [C.3.3.2.2.4]

The controls required to mitigate the risk of losing confidentiality resulting from misuse of, or unauthorized access to the system, begin with identification and authentication controls. Controls for access to Government data and Networx services information are determined on an individual basis and presented as part of the overall solution. █████████████████████

██

███

██

██

████████████████████████████████ explained in greater detail in section 2.3.3.4.),

██

██ GSA or Agency mission.

The contractor shall identify and authenticate contractor personnel and Government personnel who are authorized to place orders or to access network management information. [C.3.3.2.2.4]

Each person with privileged access to a Networx service or support system is granted access based upon the assigned responsibilities. The user's access is restricted to the minimum permissions necessary to perform normal or routine assigned tasks. Critical functions and responsibilities for administrating and managing these systems are optimally divided among different individuals to maintain consistent availability of these functions.

██

██

███

Use or disclosure of data contained on this sheet
is subject to the restriction on the title page of this proposal
AT&T Proprietary
Page 132 of 493
March 5, 2007

███

███████████████████████████████████

██

███████████████████████████████████████ The Networx Security

manager, Networx Project Manager, ████████████████████████

███

███

███

███

█████████████████

Government users accessing AT&T's **Business**Direct® web based access

portal to place orders or perform other online Networx management functions

██

███

███████████

███████████████████████ AT&T Networx Security Manager or Networx Project

Manager ██

██

████████████████████ **Business**Direct accounts, by design, are managed

██████████████ Agency █████████████ the designated Agency Administrator.

The contractor shall protect its infrastructure from any information threats or attacks (e.g., threats from hackers, criminals, and terrorist activities) carried out by domestic or non-domestic entities including subcontractors. [C.3.3.2.2.4]

AT&T takes a proactive and dynamic approach to managing the security of

our network and supporting infrastructure. ██████████████████████

███

███ AT&T

███

██

████████████████████████████ **Table 2.3.3.3-2**).

AT&T'S TECHNOLOGIES PROTECT INFRASTRUCTURE FROM THREATS AND ATTACKS	
Internet Protect	• Provides real-time data on potential intrusions and attacks. • Detects, identifies, quantifies, and locates the potential threats to AT&T's internal systems, services, and/or clients.
███████	██████████████████████ █████████ ████████████ █████████ █████████████ █████████ ██████████████████████████████
███████	██████████████████████ █████████ ██████████████ █████████ █████████████████████████████ █████

Table 2.3.3.3-2: Proprietary Technologies Protecting AT&T's Infrastructure. *These unique and innovative technologies are effective in protecting the Government's information.*

██

██

███████████████████████████████ This unique, industry-leading technology has repeatedly proven its ability to identify the full range of cyber threats as they are happening. AT&T's Security Management Team will work urgently and diligently with the other elements of the Global Network Operations Center to respond to and mitigate identified threats or attacks.

2.3.3.4   Information Assurance [C.3.3.2.2.5]

The contractor shall adhere to Federal Government accepted security principles and practices per NIST SP 800-14, or better, to protect the databases, OSS, and information processing systems that are critical for the continuous, reliable operation of its Networx services. [C.3.3.2.2.5]

To provide the discipline necessary to maintain a consistently secure and reliable infrastructure, AT&T's ████████████████████████████████ ████████████████ AT&T's █████████████████████████ ████████████████████████ This comprehensive library of policies and directives meets or exceeds NIST SP 800-14, and is applicable to all service elements, including system databases,

███, and information processing systems critical for the continuous, reliable operation of AT&T provided Networx services.

The contractor shall protect against unauthorized access to these databases, OSS, and information processing systems by entry from external communications devices. [C.3.3.2.2.5]

AT&T protects against unauthorized access to its databases, ████, and information processing systems by deploying internal and external access control mechanisms to limit access to Networx databases and systems and to support the continuous and reliable operations of Networx services. AT&T will use a combination of access control mechanisms, ████████████████ ████████████████████████████████████ ████████████████████████████ to restrict system access. All AT&T offered Networx services are protected in the same manner.

Information systems shall include but not be limited to the OSS, audio and video teleconferencing reservation systems, repositories of Agency network configuration, repositories of users' identification and authorization information and Call Detail Records (CDRs). [C.3.3.2.2.5]

AT&T's information systems in support of Networx includes all ordering, billing, inventory, network configuration, performance and service usage reporting, and trouble and complaint handling applications accessed through AT&T's secure Networx web site. █████████████████████ ████████████████████████████ ████████████████████████████ ████████████████████

Access Control - The contractor shall provide access controls consistent with Federal Government accepted security principles and practices per NIST SP 800-14, or better, to protect its OSS and switching systems from attacks via publicly accessible ports (e.g., maintenance ports). [C.3.3.2.2.5]

AT&T provides access controls consistent with Federal Government accepted security principles and practices per NIST SP 800-14, or better, to protect its OSS and switching systems from attacks via publicly accessible ports.