APPENDIX C

United States
General Services Administration

Security Plan
for
Networx

December 13, 2006

Prepared for:

United States GSA
Washington, DC 20530

Prepared by

AT&T
1900 Gallows Road
Vienna, Virginia 22182

REVISION HISTORY

DATE	VERSION	REVISION	CHANGE DESCRIPTION
10/05/2005	1.0	Draft	Initial submittal for GSA PMO review and comment
05/08/2006	2.0	Draft	Revised submittal for GSA PMO review and comment
12/13/2006	3.0	Draft	Revised document for FPR submission

TABLE OF CONTENTS

APPENDIX C

PREFACE

This security plan has two purposes: (1) to present the baseline system security plan and approach to how we will implement the security requirements for all services and Operational Support Systems provided by AT&T on Networx Universal , and (2) to describe how we plan and implement security for client Agency systems provided under individual Networx task orders. The baseline system security plan will be augmented as needed for individual systems and services provided under the Networx Universal contract.

This security plan is viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system and as such it is considered the template of the security plan created for each system supporting Networx Services, Networx and databases. Through out this document the term *system(s)* used by AT&T refers to client Agency systems and the entire spectrum of information technology, including application and support systems for the Networx Universal Contract.

The security plan delineates responsibilities and expected behavior of all individuals who access the system and demonstrates how AT&T uses planning and security controls to help protect Government information in accordance with the following:

- OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, (updated in 2000)
- Title III of E-Government Act of 2002, *Federal Information Security Management Security Act of 2002* (FISMA)

- National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*
- NIST FIPS PUB 200 (draft), *Security Controls for Federal Information and Information Systems*
- NIST FIPS PUB 140 – 2, *Security Requirements for Cryptographic Modules*

- Public Law 104-191, *Health Insurance Portability & Accountability Act* (HIPPA) of 1996
- National Security and Emergency Preparedness (NS/EP) directives as contained in Sections C.5 and C.2.1.12

AT&T complies with the Network Reliability and Interoperability Council (NRIC), Focus Group 1A Physical Security Recommendations (specifically VI-1A-05 through VI-1A-10), ANSI T1.276-2003 and Telcordia security standards. Throughout this security plan document, reference is made to the three security objectives for information and information systems: confidentiality, integrity and availability. The definitions that follow are those used by AT&T in preparation of this document. Per FIPS PUB 199, the FISMA defines them as:

- **Confidentiality** – "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]
- **Integrity** – "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]
- **Availability** – "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

To meet the security needs of a large, heterogeneous, and geographically distributed user community and protect national security, this plan for Networx uses the system life cycle approach outlined in NIST Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*. It is designed to reduce vulnerabilities, adapt to new threats, and help maintain Networx security management capabilities are updated to the latest standards and practices. 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 help protect the confidentiality, integrity and availability of Government information, databases, Operational Support Systems (OSS), and information

systems, and to support fundamental uniformity as the Government transitions to commercially managed IT solutions, Networx security is designed and implemented following the guidelines in NIST SP 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems". Agency-specific security requirements will be defined as required on a case-by-case basis as Agencies contract for services.

The security plan describes the measures that are implemented to detect and prevent security breaches, including monitoring and auditing the networks, systems, and services contracted under Networx. The objective is to minimize the impact of security breaches and attacks, as well as to minimize fraud, waste, and abuse.

Organization of Document

The sections of this document are organized to explain the activities that AT&T performs and the documents that AT&T creates to implement and operate systems in a manner that adheres to guidelines that are required in the Networx Universal Contract and follows the recommended security plan outline as stated in NIST SP 800-18.

- Section One: System Identification - outlines how AT&T describes the identification, contacts, security classification, governing laws, regulations, and policies, and individuals and organizations responsible for a system's security posture. These steps apply to both, the AT&T systems supporting Networx Services, Networx OSS, and databases and when AT&T receives a task order to develop a system for a client Agency.
- Section Two: Sensitivity of Information Handled - outlines how AT&T determines the classification of a system based on the sensitivity of the information handled by the system. Included in this section are sample tables that will be used to identify the types of information handled by a

specific system and to minimize Risk and Magnitude of Harm resulting from the loss, misuse, unauthorized access to, or modification of, information handled by the system being documented.

- Section Three: Management Controls - outlines how and when AT&T performs Risk Assessment on the systems supporting Networx Services, Networx OSS and databases. This section also describes the documents AT&T produces, the procedures AT&T follows, and the tools AT&T uses through the entire lifecycle of a system to ensure management controls are in place and follow Networx Universal Contract requirements.
- Section Four: Operational Controls - outlines the activities AT&T personnel perform and the documents AT&T creates that define how system access is granted and revoked for personnel, the methods personnel deploy to physically protect systems, methods and procedures of handling media containing government information or data, and methods of operations continuity including configuration and data backup, security patching, and disaster recover. The Operational Controls section of the security plan for a system will explain the activities AT&T performs and the documentation AT&T produces through the system's lifecycle. Finally this section outlines the methods and procedures that AT&T personnel use to respond to a security incident, including failure of a planned and implemented security control.
- Section Five: Technical Controls - outlines the activities AT&T personnel perform and the documentation AT&T creates to configure systems to automatically control access via password enforcement, control the level of access to each system by each user along with the activities each user is allowed to perform, and the firewall rules and intrusion detection system signatures used to block unauthorized access and report on failed attempts. The Technical Controls section also outlines the tracking of activity for audit purposes.

- Section Six: Supplemental Information - describes in detail the activities AT&T personnel perform and the documents AT&T creates to ensure that the security management, technical, and operational controls are in compliance with government security management requirements. The Supplemental Information section of the security plan includes a description of AT&T security management organization, security resources, strategies, policies, procedures, and security best practices which direct AT&T personnel in the execution of the Networx Universal Contract security requirements. This section outlines the type of tools used and the types of documentation AT&T provides to ensure that system risk level is appropriately determined, vulnerabilities are identified, and impact analysis is completed. The methods are described to ensure operational and technical controls are implemented correctly for Networx services and Networx OSS and databases as specified in the security plan and are producing the desired outcomes in meeting the government security requirements.

The Supplemental Information section also describes how AT&T managed suppliers, vendors, and partners ensure that personnel and security controls of these organizations adhere to the same standards and security controls AT&T personnel are required to implement. Finally, this section describes the fraud protection processes put in place to detect system abuse and how AT&T considers the security plan a dynamic document that is updated for future technologies, new and improved security methods and practices, and requirements to handle new threats to information systems.

In accordance with the requirements in section C.3.9.2.1, AT&T will ensure all security requirements are met for all automated OSS provided to support the Networx contract. AT&T will support Government certification and accreditation of the AT&T OSS via services, such as Managed Tier Security Service, Customer

Specific Design and Engineering Services, or other services the Government may order to achieve this. AT&T will include security controls for low impact systems. The attached plan will demonstrate AT&T fully understands and complies with the network system security requirements in the Networx RFP. It will also demonstrate AT&T has the personnel and processes in place to effectively manage and safeguard the data elements of systems required to support the Networx contract. Systems delivered under this contract will have the same set of security controls.

1 SYSTEM IDENTIFICATION

This security plan describes information security controls the AT&T Team routinely implements to protect systems, including networks, against security risks and vulnerabilities. This security plan does not include any sensitive or classified system information. It does, however, contain AT&T proprietary information considered to be competition sensitive. Therefore, it is marked, handled, and controlled as “Proprietary”. In addition, it is dated for ease of tracking modifications and approvals. If applicable, each unique system security plan includes the appropriate classification level and is marked and handled accordingly.

1.1 Security Plan Name/Title

AT&T begins each security plan by listing the name and title of the system/ application. Each system or application assigns a unique name/ identifier. The unique name/identifier remains the same throughout the life of the system to enable the organization to track completion of security

requirements over time. If no unique name/identifier has been assigned or is not known, AT&T will contact the appropriate security or information resource management office for assistance.

1.2 Responsible Organization

In this section, AT&T will list the federal organizational sub-component responsible for systems and services delivered under the Networx contract. If a state or local Government or contractor performs the function, AT&T will identify both the Federal and other organization and describe the relationship.

The responsible organization for the FTS Networx is:

GSA/FTX/TQC

10300 Eaton Place, Fifth Floor

Fairfax, VA 22030-2239

1.3 Information Contacts

In this section, AT&T will list the names, titles, organizations, and telephone numbers of individuals designated to be the points of contact for each system contracted under Networx. The following is an example and listing of the contacts AT&T routinely includes in each system security plan. The designated individuals will have sufficient knowledge of the system to be able to provide additional information or points of contact, as needed. Each contact will be included using the format shown below, as recommended in NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems.*

Authorizing Official:

Name:

Title:

Organization:

Address:

Work Phone:	
Email:	

Other contacts included in this section:

Certification Agent

Information System Owner

Program Manager

User Representative

The Information Contact for the FTS Networx RFP is:

Name:	John T. Braun
Title:	Contracting Officer
Organization:	GSA
Address:	10300 Eaton Place, Fifth Floor
	Fairfax, VA 22030-2239
Work Phone:	703-306-6423
Email:	jack.braun@gsa.gov

This system security plan is a broad overview. Once task orders are awarded for Networx systems, networks, and services, AT&T will identify specific responsible parties from the Government entities involved and AT&T.

1.4 Assignment of Security Responsibility

Per NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, an individual must be assigned responsibility in writing to maintain adequate security for the application or general support system. To be effective, this individual must be knowledgeable of the management, operational, and technical controls used to protect the system. In most cases, AT&T personnel are assigned security responsibilities, as are Government personnel. For instance, the Information System Security Officer and the system maintainer are generally designated AT&T personnel. As recommended by NIST SP 800-18, AT&T

customarily includes the name, title, and telephone number of the individual who has been assigned responsibility for the security of the system.

Once task orders are awarded for systems, networks, and services under Networx, AT&T will identify those responsible for security, both for the specific Government entities involved and AT&T. Security contact information will be included, in the format shown below as recommended in NIST SP 800-18, in each security plan.

The following is a listing of security contacts customarily included by AT&T in system security plans:

Information System Security Manager
Name: Contact Name
Contact Title:
Organization:
Address:
Work Phone:
E-Mail: Contact Name@att.com
This is a primary security contact for the system

Other contacts included in this section:
Information Owner
Information System Security Officer

1.5 System Operational Status

For each system under the Networx umbrella, AT&T will indicate one or more of the following for the **system's operational status**:

- *Operational* – the system is operating.
- *Under development* – the system is being designed, developed, or implemented.

- *Undergoing a major modification* – the system is undergoing a major conversion or transition.

If the system is under development or undergoing a major modification, information will be provided about methods used to include up-front security requirements. AT&T also will include specific controls in the appropriate sections of the plan, depending on where the system is in the security life cycle.

1.6 General Description and Purpose

This contract is for telecommunications services and solutions and is referred to as Networx. Networx task orders are intended to meet the program goals for:

- **SERVICE CONTINUITY**
- **HIGHLY COMPETITIVE PRICES**
- **HIGH-QUALITY SERVICE**
- **FULL-SERVICE VENDORS**
- **OPERATIONS SUPPORT**
- **TRANSITION ASSISTANCE AND SUPPORT**
- **PERFORMANCE-BASED CONTRACTS**

Within the FTS Networx Program, Agencies will generally have the right to select the acquisition that meets their requirements, to buy from multiple contracts, and to change contractors and services within the FTS Networx Program when appropriate.

The scope of each Networx task order will include all services and solutions necessary for the Government to satisfy its worldwide telecommunications and networking requirements for the life of the contracts. In addition to the specific statement of work requirements set forth in Section C of the Request for Proposals (RFP), the scope of this contract includes, at the discretion of the Government, technological enhancements, service improvements, customer-specific applications and extensions, ancillary equipment, and Customer Specific Design and Engineering services necessary to complete solutions. The scope also includes all new and/or emerging telecommunications service offerings. In

particular, the scope of each task order for Networx service will include all local, regional, national, and international telecommunications services, features, functions, software enhancements, network-based applications, and associated offerings that will be available as a part of the contractor's offerings in the commercial marketplace during the term of these contracts, plus network-based solutions and services for which there may not be commercial offerings.

1.7 System Environment and Special Considerations

In planning for security risk management for an information technology (IT) system, AT&T's first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. Characterizing an IT system establishes the scope of the risk assessment effort, delineates the operational authorization boundaries, and documents risk drivers, such as the types/models/versions of hardware and software; system/network interconnectivity; and identity and types of users.

In this section, AT&T also includes a technical overview of the system and any special security considerations. Characteristics addressed include Internet connectivity, physical environment of the systems, hardware, software, and firmware, whether the system or network is accessible to the general public, whether the system is housed outside the direct control of the owning Government Agency, and whether remote access is allowed.

The risk-based assessment methodology used by AT&T complies with NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, which can be applied to assessments of both single and multiple, interrelated systems.

1.8 System Interconnection/Information Sharing

In order for a community to effectively manage risk, it must control access to and from other systems. The degree of such control should be established in the security plan. AT&T implements such technical controls as are required to accomplish effective system boundaries to establish a logical demarcation.

There are varying degrees of system interconnectivity. AT&T and the contracting Agency will collaborate to carefully determine appropriate system boundaries for each system, network, or solution provided to the Government by AT&T under Networx.

System interconnection is the direct connection of systems for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system operators, information owners, and management obtain as much information as possible about the vulnerabilities associated with system interconnection and information sharing and the increased controls required to mitigate those vulnerabilities. The Government-designated individual and AT&T program manager will identify all system interconnections in order to make informed decisions regarding risk reduction and acceptance.

OMB Circular A-130 requires that written management authorization (often in the form of a Memorandum of Understanding or Agreement), be obtained prior to connecting with other systems and/or sharing sensitive data/ information. Under the AT&T plan, the written authorizations will specify the rules of behavior and other controls that must be maintained by the interconnecting systems for each

network or system contracted under Networx. This section contains the following information concerning authorization:

- List of interconnected systems (including Internet)
- Unique system identifiers, if appropriate
- Name of system(s)
- Organization owning the other system(s)
- Type of interconnection (TCP/IP, dial-up, SNA, etc.)
- Short discussion of major concerns or considerations in determining interconnection
- Name and title of authorizing management official(s)
- Date of authorization
- System of record, if applicable (Privacy Act data)
- Sensitivity level of each system
- Interaction among systems
- Security concerns and rules of behavior of other systems that need to be considered in the protection of this system

1.9 Laws, Regulations, and Policies Affecting the System

This section provides a listing of the laws, regulations, guidelines, and policies that establish specific requirements for **confidentiality**, **integrity**, or **availability** of the system. Each contracting Agency will decide on the level of laws, regulations, and policies to include in the security plan unique to its system or network. If a system processes records subject to the Privacy Act, the number and title of the Privacy Act system(s) of records are included along with information about whether the system(s) is used for computer matching activities.

It is AT&T's practice to comply with all applicable laws and regulations. A typical system security plan would include, but not be limited to, the following: Federal

laws, regulations, guidance, and policy pertain to the security of US Government automated information systems:

- 18 USC 1030, Computer Fraud and Abuse Act of 1986, amended 1994 and 1996
- OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, (updated in 2000)
- Title III of E-Government Act of 2002, *Federal Information Security Management Security Act* of 2002 (FISMA)
- National Institute of Standards and Technology (NIST) Special Publications, as follows:
  - SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996
  - SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model, April 1998
  - SP 800-18, Guide for Developing Security Plans for Information Technology Systems, December 1998
  - SP 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001
  - SP 800-30A, Risk Management Guide for Information Technology Systems, January 2004
  - SP 800-31, Intrusion Detection Systems (IDS), November 2001
  - SP 800-34, Contingency Planning Guide for Information Technology Systems, June 2002
  - SP 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, June 2003
  - SP 800-40, Procedures for Handling Security Patches, September 2002
  - SP 800-44, Guidelines of Securing Public Web Servers, September 2002

- SP 800-50, Building an Information Technology Security Awareness and Training Program, April 4, 2003
- SP 800-53, Annex 1, Recommended Security Controls for Federal Information Systems, February 2005
- SP 800-55, Security Metrics Guide for Information Technology Systems, July 2003
- SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004
- SP 800-61, Computer Security Incident Handling Guide, January 2004
- SP 800-64, Security Considerations in the Information System Development Life Cycle, October 2003

- NIST Federal Information Processing Standard Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- Draft NIST FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, July 15, 2005

2 SENSITIVITY OF INFORMATION HANDLED

All Federal systems have some level of sensitivity and require protection as part of the management practice. The sensitivity and criticality of the

information stored within, processed by, or transmitted by a system provides a basis for determining the value of the system and is one of the major factors in risk management. The description will provide information to a variety of users, such as the following:

- Analysts/programmers who help design appropriate security controls
- Internal and external auditors evaluating system security measures
- Managers making decisions about the reasonableness of security countermeasures

After AT&T and the Government identify the sensitivity of information handled by the system, AT&T will work with the Government to draw specifications for the security controls on a case-by-case basis for all networks, systems, and services contracted under Networx, in accordance with NIST SP800-18, *Guide for Developing Security Plans for Information Technology Systems.*

2.1 Description of Data Processed

AT&T will identify the specific data that is processed for each system or network contracted under Networx. Based upon the information the system processes and transmits, a classification such as *Sensitive But Unclassified* or *For Official Use Only* is assigned to the system.

2.2 Information Sensitivity

AT&T assigns an information sensitivity category for the system based on the FIPS PUB 199 standard. FIPS PUB 199 requires protection to safeguard data and information from unauthorized disclosure, protect data from unauthorized modification, and/or ensure that services are available to meet mission requirements.

The protection ratings determined for each of these three categories are:

- **Confidentiality** – The system contains information that requires protection from unauthorized disclosure.

- **Integrity** – The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification.
- **Availability** – The system contains information or provides services that must be available on a timely basis to meet mission requirements or to avoid substantial losses.

The criteria for rating systems are:

- **High** – a critical concern of the system; a security risk extreme enough to cause ongoing operational concerns in the event of an occurrence;
- **Medium** – an important concern; a security risk able to cause ongoing operational annoyances but not a business disruption in the event of an occurrence;
- **Low** – some minimal level of security is required; a security risk able to cause minimal ongoing operational efficiency issues but not a business disruption in the event of an occurrence, or a risk with a remote likelihood of occurrence.

A table such as the one below (**Table 2.2-1**) would be included to present an overview of the different types of data that interact with this system.

DATA TYPE	DATA SENSITIVITY	DATA SOURCE	RECEIVING SYSTEM	TRANSMISSION MODE	PROTECTION MECHANISM	INTERFACING SYSTEM C&A STATUS
All Data Types	Sensitive But Unclassified	All types	All types	TCP/IP	SSL	None

Table 2.2-1: Sample System Information Data Types.

The following table (**Table 2.2-2**) would present the estimated risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of, information in the system.

DATA TYPE	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
All Data Types	Low	Low	Low
Overall System Categorization	Low	Low	Low

Table 2.2-2: Sample System – Magnitude of Harm Matrix.

This section concludes with a summary of the system requirements for confidentiality, integrity, and availability protections along with its related level of sensitivity, the highest magnitude of harm resulting directly from loss, misuse, modification to, or unauthorized access of information on the system, and the overall sensitivity rating for the system.

3 MANAGEMENT CONTROLS

Management controls are actions taken to manage a system's development, maintenance, and use, including system-specific policies, procedures, assignment of individual roles and responsibilities, and rules of behavior. These controls are the overriding practices that must be followed by individuals on all the systems to be operated as expected.

The process and requirements discussed in this section reflect AT&T's methodology of providing management controls for general support systems. AT&T will work with the specific Agency to further specify the controls discussed here in response to a specific tasking.

3.1 Risk Assessment and Management

AT&T will conduct an initial Risk Assessment for all Networx services and Networx OSS support systems providing Government services. The Risk Assessment will be delivered within 30 days of Notice to Proceed and will be updated yearly thereafter. The yearly risk assessment will address all aspects of security as outlined in the RFP. AT&T will use the methodology set forth in NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, to conduct the risk assessments. The risk assessment template for this guideline is provided as Attachment B of this document.

Page 16 intentionally left blank.

3.2 Review of Security Controls

AT&T will follow the guidelines of OMB Circular A-130, Appendix III and NIST SP 800-18 for management, technical and operational controls 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 AT&T facilities. These controls include a security review on Networx services, Networx OSS, databases, or where Government information or Data is manually handled at AT&T facilities at least once every three years and within 6 months if significant system changes are made that affect the system's security posture. The security review will be performed by an AT&T organization which does not have managerial involvement or operational activities with Networx services, Networx OSS, databases, or manual processes for Networx at AT&T facilities or by an independent third party organization qualified to conduct a security review compliant to the requirements and guidelines stated in the Networx RFP. The security review will consist of a risk assessment, security test and evaluation (ST&E), and development of a plan of action and milestones (POA&M).

The risk assessment includes performing automated vulnerability scans. These automated vulnerability scans also support the ST&E and subsequent on-going security controls of the operational network supporting Networx services, Networx OSS, databases, and the Networx **Business**Direct® portal. These scans will be executed using available Commercial Off the Shelf scanning tools to verify that operating systems and network software are configured as specified in the security plan, are implemented correctly, operating as intended, and producing the desired outcomes in meeting Government security requirements. These scans are performed on a monthly

basis by an AT&T Security Assessment Team. AT&T will provide the results of these scans to the Government, within 60 days of a request.

3.3 Rules of Behavior

Federal regulations require rules of behavior that clearly delineate responsibilities and expected behavior of all individuals who have any level of physical or logical system access that would enable them to compromise a system's security. Representative rules of behavior are attached as Attachment A to this security plan. The rules of behavior conclude with a signature block requiring individuals to attest to the fact that they have read and understood the rules and will comply. As with the security plan itself, the rules of behavior will be edited to reflect the specific system addressed in the security plan. One other key factor will be added to the security plan, designation of an individual responsible for

managing the process under which impacted employees read and agree to abide by the rules of behavior. This individual will be responsible for, among other things, collecting and maintaining the signed forms (assuming that the rules are signed in hard copy) or electronic confirmations, for audit purposes.

3.4 Planning for Security in the Life Cycle

Although a system security plan can be developed at any point in the system's life cycle, the recommended approach is to create the plan at the beginning of the system development life cycle. The AT&T model for the Information Technology (IT) system life cycle contains five phases:

1. Initiation
2. Development/Acquisition
3. Implementation
4. Operation/Maintenance, and
5. Disposal

Each phase in the security risk management life cycle is summarized below, following NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*. This section will discuss the security planning that has been done to date and the activities that must be accomplished in the succeeding phases.

3.4.1 Initiation Phase

In the life cycle Initiation Phase, the need for the system is expressed and the purpose documented. Key tasks to be accomplished in the Initiation Phase are:

- Categorize the system for confidentiality, integrity, and availability
- Define security goals
- Prepare initial risk assessment and security plan
- Obtain adequate budgetary resources for IT security requirements

The Initiation Phase kicks off with the system security categorization, which is the basis for identifying system security goals and initial selection of security controls. Using a methodology based on the FIPS PUB 199 guidance, the AT&T team will categorize systems for which they are responsible. They will categorize systems as low-, moderate-, or high-impact for security confidentiality, integrity, and availability.

Based upon the categorization, a system's security goals and initial security control requirements will be defined and then reflected in the risk assessment and security plan, which also are prepared in this phase.

3.4.2 Development/Acquisition Phase

The system is designed, purchased, programmed, developed, and/or constructed in the Development/Acquisition Phase. AT&T complies with NIST's information security steps for this phase and are outlined as follows:

- Identify security requirements.
- Identify appropriate security controls and develop associated evaluation and test procedures. Ideally these steps are taken before the system procurement action so that the following step can be taken.

- Include security requirements and evaluation/test procedures in solicitations such as RFPs.
- Provide flexibility in the security planning process so that security requirements can be updated as new threats/vulnerabilities are identified and as new technologies are implemented.

As noted above, these steps may be necessary for a system that is well past the system development/acquisition phase of its life cycle if not completed at the appropriate stage.

3.4.3 Implementation Phase

In the Implementation Phase, the system's security features are configured and enabled, the system is tested and installed or fielded, and the system is authorized for processing. The principal Information Assurance (IA) activities of the Implementation Phase are as follows:

- Conduct the ST&E and supporting vulnerability scans
- Identify and mitigate vulnerabilities
- Update the risk assessment and security plan
- Prepare the documentation in adherence with NIST SP 800-37 guidelines.

The IA focus of the Implementation Phase is to ensure adherence with NIST SP 800-37 guidelines:

- The ST&E completed to verify that all required security controls are in place and functioning as designed.
- The final risk assessment is completed, based on the outcome of the testing.
- Any changes in the system and its security requirements and controls that have occurred since the Development Phase are documented.

If the ST&E and scans identify unacceptable security risks, then POA&M developed to identify vulnerabilities that must be mitigated, assign responsibility

and a schedule for remediation activities, and describe the process for monitoring and verifying the necessary corrective actions.

With completion of the documentation, including the security plan, risk assessment, configuration management plan, and other documentation necessary to demonstrate the system's security posture, the AT&T team will assemble the documentation and present them to the appropriate Designated Approving Authority (DAA).

3.4.4 Operation/Maintenance Phase

After the system has been successfully deployed, it enters the Operations and Maintenance (O&M) Phase. During this phase the system becomes operational and any necessary system modifications are identified and documented as *System Change Requests*. System changes must be formally approved before they can be implemented. IA activities in this phase include the following:

- Conduct annual user security awareness training
- Review C&A status as needed, including conducting the annual self-assessment
- Review and update the security plan annually, or more frequently if security-significant system changes are made
- Conduct risk assessments as required; identify and mitigate vulnerabilities
- Execute scheduled and unscheduled vulnerability scans
    - Maintain and annually test the contingency/disaster recovery plan

3.4.5 Disposal Phase

The Disposal Phase of the IT system life cycle involves disposing of information, hardware, and software when they come to the end of their life cycle. The information assurance issue that must be considered is secure disposal of any sensitive information. The first consideration will be the disposal of information, whether it will be moved to another system, archived, discarded, or destroyed. Sensitive material will be destroyed. However, the exact and appropriate method will depend upon the sensitivity of the specific system. Similarly, degaussing, sanitization, and/or destruction are usual means of destroying sensitive magnetic media.

Another consideration is the disposition of network devices. Any equipment used to store, process, or transmit information must not be released from its physical site until the equipment has been sanitized and cleared of all information.

3.5 Authorize Processing

The client Agency designates a DAA for the system for which AT&T is assigned responsibility through a Networx task order. That DAA will grant authorization for the system to go into production. System authorization is required by OMB Circular A-130 as a means to make management aware of the identified risks associated with a general support system and that they accept any residual risk that remains after reasonable controls are implemented. Individual Agencies have similar and supporting system authorization requirements.

4 OPERATIONAL CONTROLS

The operational controls address security mechanisms that focus on methods that are primarily implemented by people, as opposed to those implemented by systems. They often require technical or specialized expertise and often rely on management activities as well as technical controls.

4.1 Personnel Security

This section describes the controls required to mitigate the risks of system harm/disruption resulting from both the intentional and unintentional actions of persons with authorized access to the system. These controls begin with restricting access to appropriate personnel and that access is restricted to no more functionality than each person needs to execute their assigned role, as outlined in the NIST guidance. Personnel security also includes controls to trace user activity back to each user and established procedures for maintaining the security of the system when personnel who have had access no longer require that access.

The depth, breadth, and rigor of the personnel security controls required for a system vary depending on numerous factors, including the system's sensitivity and the owning Agency's unique regulations. The following subsections represent a scenario that somewhat typifies the Personnel Security section of an AT&T security plan. It will not be used off the shelf for any system for which an Agency contracts for support under Networx. Like all other security plan sections, it will be customized to reflect the requirements of a specific system in a specific Agency.

4.1.1 Personnel Security Management

Upon receiving a task order, AT&T will designate an individual whose role includes coordinating the aspects of the task order that pertain to obtaining and maintaining security clearances at the appropriate levels for contractor personnel.

That individual's responsibilities will include such activities as obtaining and maintaining security clearances and related coordination with the client and monitoring approvals for persons with physical access to sensitive facilities. AT&T's security office currently initiates/processes an average of [redacted] security clearances monthly.

4.1.2 Sensitivity of Positions

The sensitivity of positions that require system access will depend on the classification level of the system. There are expected to be two classifications of users,1) privileged administrative users, such as system administrators, and 2) generic users

Work performed under Networx task order(s) may fall within one or more of the risk categories defined below. Therefore, AT&T personnel will undergo background investigations commensurate with the risk factor associated with the duties of each position.

- **High Risk** positions have the potential for *exceptionally serious* impact involving duties especially critical to the system-owning Agency. These may include computer positions responsible for planning, directing, and implementing the system's security program; directing, planning, and designing the system, including the hardware and software; or accessing the system during its operation or maintenance in a way that would enable them to cause grave damage or realize significant personal gain.
- **Moderate Risk** positions are *sensitive* positions that have the potential for *moderate to serious* impact involving duties very important to the system-owning Agency. These may include computer positions of a lesser

degree of risk than seen in High Risk positions, as defined in OMB Circular A-130, Appendix III.

- **Low Risk** positions are non-sensitive positions that do not fall into either of the preceding categories and include those positions with potential for impact involving duties of *limited relation* to the system-owning Agency's mission.

4.1.3 Required Background Investigations

Background investigations will be conducted and favorably adjudicated for all contractor personnel before they begin work on a task order if applicable. Typical minimum pre-appointment investigative requirements are as follows:

- **High Risk** positions may require a Limited Background Investigation (LBI), which consists of a personal subject interview, National Agency Check (NAC), credit history check, written inquiries, record searches covering five years, and personal interviews covering specific areas during the most recent three years.
- **Moderate Risk** positions may require a National Agency Check and Inquiries (NACI), which consists of written inquiries and record searches covering specific areas of a subject's background during the preceding five years.
- **Low Risk** positions may require a Federal Bureau of Investigation (FBI) Name and Fingerprint check.

Generally, AT&T Government Solutions' Security Office facilitates compliance with background investigation requirements.

4.1.4 Pre-Appointment Background Investigation Waivers

Depending upon the client Agency's requirements for the task order, the Agency may be unable to wait for an entire background investigation to be completed. In such cases, it is common for a pre-appointment background investigation waiver to be granted. The extent of the background investigation needed to qualify for waivers varies by Agency, system sensitivity, and position sensitivity. Typical waiver requirements are as follows:

- **High Risk** positions may require a successful National Crime Information Center (NCIC) check, vouchering of previous two employers, and a favorable review of forms submitted.
- **Moderate Risk** positions may require a favorable NCIC check and a favorable review of forms submitted.
- **Low Risk** positions may require a favorable NCIC check.

As with the background investigations, the AT&T Government Solutions' Security Office generally is responsible for facilitating waiver requirements and coordination with the client Agency.

4.1.5 Required Security Forms

AT&T employees holding sensitive positions supporting Federal Agency systems generally complete the following forms:

- Applicant Fingerprint Card (FD-258) – two sets per applicant
- Questionnaire for Non-Sensitive Positions (SF-85), or Questionnaire for Public Trust Positions (SF-85 P)

AT&T currently has approximately [redacted] cleared personnel. AT&T [redacted]

4.1.6 Operational Access Controls

Each person with access to a Networx system will be granted his or her access based upon their assigned responsibilities, with each user's access restricted to the minimum necessary to perform their assigned duties. Where possible, critical functions will be divided among different individuals; where impractical, variations from this requirement will be justified and documented. This division, or separation of duties, will be established and maintained through access controls. Where possible, necessary administrator access must be granted through user accounts rather than through root access.

Assignment of user privileges will follow the client Agency's protocols for requesting, establishing, issuing, and closing user accounts. The AT&T project manager or her/his delegate will provide oversight for access requests and approvals. AT&T will develop standard access control documentation that will be used to document access requests, justifications, and approvals. In addition, all AT&T personnel assigned to a Networx task order will comply with the client Agency's security policies and procedures, sign the rules of behavior, and follow those procedures developed for the operation and maintenance of the Networx system.

For AT&T personnel, AT&T checks activity status of all user accounts on a daily basis. User accounts that have been inactive for 45 days are deactivated and user accounts that have been inactive for 120 days are deleted.

For Government personnel, their ability to place orders or to access network management information is driven via access to the **Business**Direct® portal. AT&T works with each Government Agency to establish an administrator for the **Business**Direct user accounts. The Agency administrator is responsible for establishing, maintaining and deleting accounts within that Agency. This provides the Agency with control over their information access. **Business**Direct does not automatically make user accounts inactive and does not automatically delete them Controls within **Business**Direct require that user account passwords expire after 180 days. Users must update their account password prior to accessing the system if the password has not been chaged within the 180 day period.

4.1.7 Holding Users Responsible for their Actions

Two mechanisms will be in place for holding users responsible for their system-related actions:

1. The attached rules of behavior will be customized for the contracted system and disseminated to everyone with any physical and/or logical access to the network. Each such person will sign a copy of the rules to acknowledge receipt, and the project manager or her/his delegate will maintain the signed documents.
2. The security audit capability and processes described below under *Audit Trails* will be implemented and maintained. Each system user will have their own account, with a unique login ID and password, and all security-

related user activities will be logged. Because each user must have a unique account, there will be an audit trail of each person's activities. As discussed in the *Audit Trails* section, to provide the opportunity to identify any suspicious activity, specific individuals will be designated as responsible for reviewing the administrator activity logs periodically.

4.1.8 Friendly and Unfriendly Termination Procedures

Upon termination or transfer of personnel from duties related to the contracted system environment, whether the person's departure is friendly or unfriendly, the AT&T project manager or her/his delegate will ensure that system access is terminated.

Judgment will be exercised in deciding upon the timing of terminating access. In the case of unfriendly terminations, system access will be terminated immediately. If an employee is to be fired, system access will be removed just before or at the same time the employee is notified of their dismissal. If an employee gives notice of resignation and it is suspected that it may be on unfriendly terms, system access also will be terminated immediately.

As part of the AT&T employee's exit interview, or at an earlier time if appropriate, the departing employee will, in addition to the usual AT&T exit procedures, be briefed on their responsibilities for confidentiality and privacy with respect to the Networx task orders in particular and explicit direction must be given relative to what information they are allowed to share with different classes of individuals, such as the person's co-workers and the public.

Also, as part of the employee's exit interview, or at an earlier time, all tangible access tools, such as authentication tokens and key cards for facility doors, will be retrieved and accounted for. In the case of an unfriendly termination, any cipher lock combinations must be changed, and any keyed locks must be re-keyed upon the employee's departure.

4.2 Physical and Environmental Protection

AT&T currently provides or will provide the following controls, in accordance with the corresponding NIST guidelines, for each physical site where system devices, media, or other resources are housed:

- Site plans detailing responses to emergencies for IT facilities.
- Annual reviews of physical security measures.
- Controlled physical access through the use of guards, identification badges, or entry devices such as key cards or biometrics.
- Keys or other access devices required to enter these sites, including data center(s), computer room(s), and tape/media libraries.
- Properly-secured keys or other entry devices that are not issued. A specific Networx task order will specify where and how these devices are secured and the individual(s) responsible for maintaining and issuing entry devices.
- Cipher lock entry codes changed periodically, if cipher locks are used to physically secure these sites. The schedule and off-schedule times at which codes are changed and the individual(s) responsible for ensuring that codes are changed as specified.
- Authentication of visitors, contractors, and maintenance personnel who may access these sites. Authentication is done through the use of preplanned appointments and identification checks.
- A procedure for signing in and escorting site visitors. A register is maintained that includes the names of the visitor and the person authorizing the visit, visitor signature, date, and time in and out.
- Emergency exit and re-entry procedures to ensure only authorized personnel can re-enter after fire drills and any other similar mass departure/re-entry of the site.

- System cabling and other communications equipment closets physically secured to prevent unauthorized access.
- Physical access to routers, switches, telephony gateways, routers, and other sensitive equipment restricted to trusted authorized personnel.
- All perimeter walls and firewalls extending from the structural floor to the structural ceiling.
- Neither interior nor exterior windows opening into a non-secured area.
- Environmental protection for IT systems. The means of providing the protection will be documented.
- Appropriate fire suppression and prevention devices installed and functioning.
- Reviews for fire ignition sources, such as failures of electronic devices or wiring, improperly stored materials, and the possibility of arson are performed in accordance with each AT&T operations facility and their documented fire code procedures. The frequency of inspections varies with the fire code that applies to the location and by the type of equipment being inspected. The AT&T Oakton, VA and Kansas City, MO facilities that support the Networx OSS, databases, and **Business**Direct® portal applications have inspections performed at intervals ranging from "continuously" to "annually", in adherence to local fire codes. At the Oakton facility, AT&T conducts the following reviews at frequencies as indicated in **Table 4.2-1**:

TYPE OF REVIEW	FREQUENCY
Electronic Monitoring of facility's fire system by external company	Continuously
Walk-through of facility by security patrol to detect breaches including indications of fire	Nightly
Sprinkler System testing	Quarterly
Test of fire hydrants	Semi-Annually
Testing of facility fire control system	Annually
Fire pump/rooftop flow testing	Annually
Inspection of tamper and flow switches	Semi-Annually
On-line Building Emergency Action Plan for Tenant review of notification and call out procedures	Annually
Inspection by Fairfax County Fire Marshall	Annually

TYPE OF REVIEW	FREQUENCY
Fire extinguisher inspection	Monthly
Kitchen Hood suppression inspection	Semi-Annually
Fire Drills conducted	Twice a year
Fire safety inspection report by Facility Manager	Monthly

Table 4.2-1: Fire Prevention Protects Networx Facilities. *AT&T performs reviews to ensure protection for the Government's Networx services.*

- Cables leaving and entering the site installed with fire stops.
- The temperature and humidity within the facility monitored and controlled to provide an operational environment that conforms to the manufacturer specifications.
- Heating and air-conditioning systems maintained regularly.
- A redundant air-cooling system for the site(s).
- Building plumbing lines identified.
- Reviews of electric power distribution, heating plants, water, sewage, and other utilities.
- Power circuits clearly identified, dedicated, and meeting equipment manufacturer amperage requirements.
- Equipment that is grounded with American Wire Gauge (AWG) #6, meets manufacturer's specifications, and complies with local electrical code.
- An uninterruptible power supply (UPS) or backup generator(s) to back up the system in the event of AC power failure. The UPS or generator(s) achieves a minimum of one hour of power backup.

- Equipment cabinet doors that remain locked.
- Controls to mitigate effects of other disasters, such as floods and earthquakes.
- Network administration terminals with the following safeguards: physically located to minimize unauthorized access or viewing; password control and password aging features invoked; timed auto logoff enabled, and protection from unauthorized use.
- A risk analysis that considered additional environmental and physical controls for facilities that support large-scale IT operations, such as telecommunication facilities.

4.3 Production Input/Output Controls

The production input/output controls maintain the security posture of a system's live processing environment and appropriately distribute its data. These controls include help desk and other user support and are used for marking, handling, processing, storage, and disposal of input and output information and media. These controls are also used for labeling and distribution procedures for the input and output information and media. These controls include the mechanisms used to monitor the installation of and updates to the production environment.

4.3.1 Marking and Storing Devices and Media

AT&T protects system devices and electronic media by marking them in accordance with the system's sensitivity and to the highest classification level authorized (e.g., Limited Official Use). System devices contain external classification markings authorizing the level of information that can be processed. Data is not stored on electronic media that cannot be adequately secured against unauthorized access.

4.3.2 Device and Media Disposal

System devices that have processed, stored, or transmitted sensitive information will not be released from system control until the equipment is sanitized and all stored information has been cleared. For sensitive information, the sanitization method will be approved by the client Agency and documented in the customized security plan. If any system IT equipment is maintained under warranty contracts, the contracts will include stipulations that equipment removed from its hosting site will be sanitized before its removal.

When no longer required for system support, IT storage media to be re-utilized for unrelated system purposes will be overwritten with software and protected consistent with the data sensitivity and/or at the highest classification level at which they were previously used. If the system processes, stores, or transmits classified data, then classified media will be disposed of in accordance with measures established by the National Security Agency (NSA) and the required disposal procedures of the client Agency.

Official electronic records will be properly disposed of and, if appropriate, archived. AT&T will identify any official electronic records related to the system and the approved disposal/archive procedures to be followed.

The Networx Security manager or her/his delegate will maintain records regarding all aspects of the implementation of disposal actions and verification the device or media was sanitized in accordance with NIST guidelines.

4.3.3 Monitor the Production Environment

Production, input/output controls include the mechanisms used to monitor the installation of and updates to the production environment.

A ST&E will be developed and executed to validate that security requirements for contracted systems, Networx services, Networx OSS, and databases are satisfied. The ST&E will test controls as prescribed as well as compliance with

secure operating system configuration requirements tested using one or more automated security scanning tools. As part of the ST&E, and annually or within six months after there is a significant change to the environment that alters the in-place assessed risk thereafter, the system will be reviewed to identify and eliminate unnecessary services, ports, and protocols.

The system will be reviewed annually or within six months after there is a significant change to the environment that alters the in-place assessed risk for known vulnerabilities, and software patches will be installed. AT&T will specify the process by which the system will be reviewed including schedule, tools, methods, and responsible personnel. AT&T will also specify procedures for identifying, downloading, testing, and applying patches, service packs, and hot-fixes.

The use of any copyrighted software will be documented. Shareware and personally-owned software/equipment will require a waiver and will be documented. AT&T will include procedures under which any copyrighted software will be used in compliance with applicable copyright laws and will be incorporated into the system's life cycle management process.

Other system configuration requirements are as follows:

- Laptops and mobile computing devices (including personal digital assistants [PDAs]) approved for processing sensitive information will not be connected to networks or systems unless the network or system is designed for that functionality. The devices will employ virus protection software and encryption technology.
- Automatically forwarding e-mail regardless of the forwarding method employed either to the system or through the system if it is a network, is forbidden unless the DAA grants a waiver.

4.4 Contingency Planning

Critical Networx services configurations and Networx OSS data and information generated and stored at AT&T Networx facilities will have a NIST-compliant contingency plan in place throughout the length of the Networx contract period to facilitate continuity of system functions in the event of disruption in computer operations. These contingency plans, also referred to as disaster recovery plans or business recovery plans, will include steps taken to ensure preparedness, including near real-time, mirrored back-up of all servers at off-site locations and plans for timely response after a disruption. This process will be applied to systems that support critical Networx services, Networx OSS, and databases. .

4.4.1 Continuity of Operations Plans

Three essential contingency planning activities will be combined to provide for plan-related testing, training, and management approval. The plan will be tested and revised as necessary based on the testing. The plan will be tested using the tabletop approach. Using this approach, all personnel expected to implement any part of the plan will be assembled and, using a facilitated workshop methodology, walk through multiple contingency scenarios, validating the steps described in the plan. While the plan may require revision based on the testing, the individuals responsible for executing the plan will have been trained in their responsibilities by participating in the testing scenarios. Additionally, the approval of the key affected parties will be gained through the process.

After revisal, the plan will be distributed to the personnel responsible for executing the plan. Once implemented, the plan will be tested annually or within six months after a significant change to the environment that alters the in-place assessed risk of the affected system.

4.4.2 Backup and Off-Site Storage

Day-to-day security operations and administration include performing regularly scheduled software backups and managing the backup media. Recent software and data backups would be essential if it became necessary to recover from a disaster, whether it is a natural disaster, such as a fire or flood; a crime, such as an intruder's vandalism of the network or a supporting computer facility; or a hardware or software failure or user error. Duplicate backup media must be stored off site, in accordance with NIST guidelines, to minimize the risk of being damaged or destroyed with the production environment.

AT&T will ensure offsite backup and storage of critical Networx services configuration, OSS data, **Business**Direct® portal, and information stored at its Networx facilities. On a regular basis as part of normal operating procedure AT&T OSS data and services configurations, including those that will specifically be used to support the Networx Universal Contract, are backed up on a mirrored server. These back-ups servers are located at a different site from the primary server location. Each site and storage server follows specific back-up and recovery plans that are documented and tested regularly

Alternate storage site(s) will be geographically removed from the primary site(s) and physically protected at the same level that the primary site(s) are protected. During non-duty hours, sensitive information will be provided some minimum storage protection, such as secured in a locked file cabinet or stored in a facility with physical access control measures.

4.5 Hardware and System Software Maintenance Controls

Hardware and system software maintenance controls help to accomplish maintenance, repairs, upgrades, and enhancements without adversely affecting the network's security. These controls are used to monitor the

installation of and updates to hardware, operating system software, and other software to assess whether the hardware and software function as expected and to maintain a historical record of changes.

4.5.1 Maintenance and Repair

AT&T will develop on-site and off-site maintenance procedures. The procedures will include restrictions on who may perform maintenance and repair activities, guidelines and procedures for escorting maintenance personnel who need to work in restricted areas, and securing devices or removable media that must be removed from the site. The capabilities to add, change, or remove system devices, dial-up connections, and network addresses and protocols or to remove or alter programs will be restricted to authorized personnel, as described in the *Personnel Security* and *Logical Access Controls* sections.

4.5.2 Configuration Management

A configuration management process will be in place and documented to maintain control of system changes and to provide a current history of system change. AT&T will prepare a system configuration management plan. The plan will identify the personnel responsible for system configuration management as well as the guidance and procedures for configuration management. In accordance with NIST guidelines, AT&T will address the following requirements:

- Software change request forms to document requests and related approvals
- Review, evaluation, and approval of every documentation, hardware, software, and firmware change request before changes can be made
- Documented and archived authorizations for all modifications
- An impact analysis to determine the effect of proposed changes on existing security controls, including required training needed to implement the control

- Procedures for testing all changes before modifying the accredited production system so that new information security vulnerabilities are not introduced into the operational environment
- Revised approvals, after testing and documentation, to migrate changes into the production environment
- Emergency change procedures and the personnel authorized to approve an emergency change. Emergency changes will be documented and approved by management, either prior to the change or after the fact.

The configuration management plan also will specify procedures and documentation requirements for maintaining version control over production software and hardware, labeling and inventorying software, and distributing and implementing new or revised software.

4.6 Integrity Controls

Integrity controls protect the system and the data it processes, stores, and/or transmits from accidental or malicious alteration or destruction and provide assurance to the end user that the information meets expectations about its quality and that it has not been altered. Validation controls are tests and evaluations used to determine compliance with security specifications and requirements. The system security requirements and controls that fall within this category are described in the following sections.

4.6.1 Virus Control

AT&T will work with the client Agency to develop an appropriate virus management policy that complies with the Agency's policy. AT&T understands anti-virus software is most effective when kept current, and, therefore, will stress procedures for maintaining current anti-virus signatures in the policy.

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 OSS or service providing systems:

- Install the latest version of the corporate licensed anti-virus software designated by Network Security for AT&T use
- Options of automated anti-virus software to maintain current protections are not disabled or modified
- Run the anti-virus software on all local drives and all removable media maintained by the user
- Scan all network shares owned by the user
- Scan all files that have been downloaded or copied from email messages or the Internet
- Perform regular back-ups (preventing all data from being lost in case of pervasive virus or catastrophic attack)
- Use only Company authorized (i.e., purchased, owned, leased, or management-approved, personally owned) software on Company computers (software used on Company machines must not be pirated and must be free of malicious code or viruses that could result in the loss of Company data).

4.6.2 Message Integrity

AT&T will support all government efforts to protect the integrity of messages in transit where these messages are protected by encryption methods including site to site VPN or SSL VPN services. Also where government data classification of systems is required, AT&T will support the use reconciliation routines such as checksums, hash totals, or record counts to protect the receiver from malicious changes to a message by confirming a transmitted message has not been altered in transit.

4.6.3 Use of Mobile Code

If there is no operational need to download mobile code or executable content, then the system will be configured to prevent downloading mobile code or executable content. Downloading mobile code and executable content from a controlled interface between interconnected systems will be permitted only when boundary protection devices are appropriately configured and will be approved by the client Agency. If mobile code or executable content is obtained via the web, the following will be applied:

- All mobile code or executable content employed within the system will be approved by the client Agency.
- A code review and quality control process for deploying mobile or executable content will be implemented and documented.

4.7 Documentation

Documentation is a security control explaining how software/hardware is to be used and formalizes security and operational procedures specific to the system. System documentation includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to the automated information system security, including backup and contingency plans and

descriptions of user and operator procedures. Typical system-related documentation is listed below:

- A system security plan
- System-specific rules of behavior
- System risk assessment report
- Vendor-supplied documentation of purchased hardware and software
- Network diagrams and documentation on setups/configuration of routers and switches
- Justifications and management approval to use copyrighted software, shareware, or any personally owned software or equipment
- Application documentation for any in-house applications
- Software and hardware testing procedures and results
- Standard operating procedures for equipment and system interfaces
- User manuals
- Emergency procedures
- Configuration management plan
- Emergency change procedures such as procedures for emergency changes to system software
- Log of distribution and implementation of new or revised software
- The system contingency plan, including backup procedures
- Written agreements regarding how data is shared between interconnected systems

4.8 Security Awareness & Education

All AT&T personnel supporting Networx systems, Networx OSS, and databases, must complete initial Security Training and an annual refresher course. The initial training is performed in person or via web-based courses. The web-based based training requires a knowledge test upon completion to ensure the individual took and understood the training. The AT&T Security Manager ensures 100% participation by employees. This training will include Networx security policies, practices, and procedures.

Security awareness is communicated to Government users via Service Introduction Packets and Best Practices information brochures. The Networx subscriber web-site will include information about Networx security policies, practices, and procedures.

AT&T's vendors are contractually obligated to comply with company policy as well as Government requirements in support of the Networx contract. AT&T's Networx Security manager ensures that the appropriate Vendor and Contractor personnel are trained on the security policies and procedures as required. Contractor personnel who perform specific security roles, such as system administrator, security administrator, and database administrator, will undergo additional specialized training focused on their respective role.

In addition, all personnel with physical and/or logical access to a client Agency's system will (1) receive the system rules of behavior, a copy of which will be signed and

returned to the designated custodian, and (2) have access to applicable client Agency security procedures and policies.

4.9 Incident Response Capability

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. FISMA and OMB Circular A-130, Appendix III, require each Agency's users of general support systems have access to an incident response capability to provide help when a security incident occurs and to share information concerning common vulnerabilities and threats.

A formal incident response capability will be available and exercised at least annually. The capability and supporting procedures will be documented. The capability will include the following:

- Security incident monitoring and tracking procedures, including how to recognize and handle security incidents and procedures for revising the incident handling procedures after an incident occurs.
- System performance monitoring procedures to be used to analyze network performance logs in real time to look for availability problems, including active attacks.
- Reporting to the appropriate emergency response.
- Receiving and responding to alerts and advisories. A process will be developed to identify the sources of alerts and advisories to be monitored, the personnel responsible for monitoring and responding to alerts and advisories, and response guidance.
- Designating the individual(s) responsible for testing and maintaining the incident response capability.

5 TECHNICAL CONTROLS

Technical controls are those executed by the computer system. Technical controls must be implemented to provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls always requires significant operational considerations and must be consistent with the management of security within the organization.

5.1 Identification and Authentication

This section describes the controls required to mitigate the risks of loss of confidentiality resulting from misuse of or unauthorized access to the system. These controls begin with ensuring users identify themselves to the system and are authenticated prior to obtaining access to perform actions on the system. Identification and authentication controls ensure users are authorized to access the system. This section represents a scenario that typifies the Identification and Authentication section of an AT&T security plan. It will not be used off the shelf for task orders under Networx, but will be customized to reflect the requirements of a specific system in a specific Agency.

The first step is to determine the method of authentication and develop procedures and policies to enforce this method. For instance, if passwords are used, then the procedures and policies would be as follows:

- The System Administrator issues the initial password.
- The initial password expires at the time of its first use and the password owner must supply a new password.

- Passwords cannot be the same as the user ID and must have at least three of the following: English uppercase, English lowercase, numerics, and special characters.
- Minimum length of eight characters permitted.
- Passwords expire every 90 days (enforced by the system).
- Expired passwords disallowed after 6 generations.
- User accounts disabled after no more than three consecutive invalid attempts (must be reinstated by an administrator).
- Vendor-provided default passwords disabled or changed.
- No shared accounts, including guest and training accounts, are defined.
- No clear text display of passwords allowed on the screen.
- Passwords stored as a hash or with one-way encryption.
- System administrator passwords transmitted and stored with one-way encryption to prevent anyone from reading the clear-text version.
- Passwords, IDs, or application user codes must not be entered in a file or record maintained in the system for the purpose of logging on automatically.

Depending on the system sensitivity, the Agency's requirements for strong authentication, and other factors, the customized security plan may specify stronger authentication tools, methods, and procedures (such as the use of one-time passwords).

5.2 Logical Access Controls

Logical access controls are the protection mechanisms that limit users' access to information and restrict their forms of system access to what is appropriate for them. These controls include policies that determine a user's level of system access, the procedures by which users are authorized appropriate access, the requirements for monitoring and maintaining access controls, and the system's technical features that enforce logical access controls.

5.2.1 User Authorization

Each user's access to a Networx system contracted to AT&T will be restricted to the fewest privileges that the user needs to perform their assigned duties. Where practical, critical functions will be divided among different individuals; where not practical, any variations from this requirement must be documented. There will be no shared administrative user accounts. Each privileged user has a personal account, so that all administrative activities are auditable.

There will be a formal process for requesting, establishing, issuing, and closing user accounts. An access control form will be developed to document access requests, justifications, and approvals. Compliance with requirements for least privilege, separation of duties, and unique accounts will be fully documented as part of the justification provided on the access control form.

A Government-designated individual must approve access privileges. The access control process requires this individual review the Access Control Lists not less than twice yearly to ensure that accesses are current and appropriate. All inactive accounts must be deleted to prevent unauthorized access, and permissions must be changed to reflect any changes in a user's assigned duties.

5.2.2 Protection from Unauthorized Access

This section addresses controls such as firewalls and intrusion detection systems (IDS) that may be implemented to counteract the threat of unauthorized system access. For Networx systems and/or networks with firewall and/or IDS protection customized for that particular system or network, AT&T will describe the related measures to help protect the system in a secure enclave.

AT&T will identify any firewalls, IDS, and other devices installed to protect the system/ network's

perimeter. We will also describe the configuration of those devices. Generally, firewalls are to be configured to exclude any traffic except that which is specifically allowed. Any exceptions will be justified and documented. The IDS are to be configured to monitor site traffic for potential misuse or policy violations and recognize patterns of misuse, such as suspicious or unauthorized activity.

Other controls to protect Networx systems from unauthorized access include secure configuration of system devices by removing access to unneeded and unnecessary services from operating systems. Such unneeded or unnecessary services might include file transfer protocol (FTP), Telnet, compilers, and software development tools, if they are deemed to present security vulnerabilities in a specific situation.

5.2.3 Public Access Controls

If a client Agency's Networx system task order provides for public access, AT&T will address the additional security controls needed to protect the integrity of the system and the confidence of the public in the system. Such controls include segregating information made directly accessible to the public from official Agency records. Other controls AT&T has designed into Federal Government public-facing web sites include the following:

- Some form of user identification and authentication
- Digital signatures to enhance authentication
- Access control to limit what the user can read, write, modify, or delete
- Controls to prevent public users from modifying information on the system
- CD-ROM for on-line storage of information for distribution
- Verify programs and information distributed to the public are virus-free
- Audit trails.

5.2.4 Warning Banner

The *Computer Fraud and Abuse Act* of 1986 (Public Law 99-474) requires that a warning message be displayed notifying unauthorized users they have accessed a U.S. Government computer system and unauthorized use can be punished by fines or imprisonment. Although some Federal Government systems, such as FirstGov.gov, are intended for unrestricted use by the general public (a situation not prevalent when Public Law 99-474 was enacted), all systems that input, process, or store Government information must comply with the law.
Therefore, for all access to a Government system, with the exception of public requests for site content which will include the warning message cited in Section III.8, an approved Agency warning banner will be displayed on all servers prior to user access, as required by NIST guidelines. As sample log-on banner is provided.

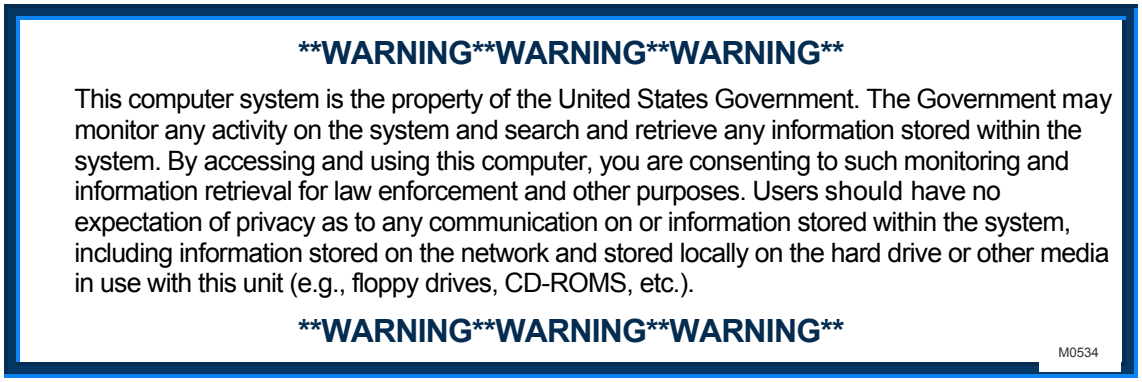

Figure 5.2.4-1: Log-on Banner. *Example of Government banner displayed at log-on.*

5.3 Audit Trails

Technical security includes controls to trace user security-related activity back to each user. Audit trails maintain a record of activity by system or application processes and by user activity. In conjunction with appropriate tools and

procedures, audit trails can support several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.

To increase individual accountability, each user must have his/her own account, with a unique login ID and password (accounts must not be shared), and all privileged user activities will be logged so audit data will be available for review. Where possible, necessary administrator access must be granted through user accounts rather than through root access.

Since each user's security-related activities will be subject to recording and routine review for inappropriate activities, audit trails must be of sufficient detail to facilitate reconstructing events if compromise or malfunction occurs or is suspected. To produce audit trails with sufficient detail, audit logs will record the following, at a minimum, for each device:

- Identifier of each person accessing or attempting access
- Date and time of the access (or attempted access) and of log off
- Activities accomplished or attempted while logged on.

The audit logs must be secured. Access to online audit logs must be strictly controlled, preferably through separation of duties between system administrators who administer the access control function, for example, and those who administer the audit trail. AT&T will identify the individual(s) responsible for reviewing security activity logs and the frequency of their reviews.

Furthermore, the individuals responsible for information security must review the audit trail following a known system software problem, a known violation of existing requirements by a user, or any unexplained system or user problem. The individuals responsible for these audit-related tasks will be identified for each client Agency task order.

6 SUPPLEMENTAL INFORMATION

The purpose of this section is to repeat certain points made in the foregoing sections, organized by topic, as raised in the Networx RFP. AT&T's security management, technical, and operational controls as well as our compliance with Government security management requirements, are highlighted.

6.1 AT&T Security Management Organization

In order to meet critical Government security requirements, AT&T maintains comprehensive security organizations at corporate and worldwide levels. These organizations are dedicated to the physical and logical security of the AT&T global network and its support systems and service offerings. These organizations review and assess AT&T's information security posture to determine whether industry security developments and evolving regulatory and business requirements have created a need for change or development. Among these organizations are:

- AT&T's Security Center of Excellence (SCOE), an organization that establishes policy and requirements, as well as comprehensive programs, to incorporate security measures into every facet of AT&T's computing and networking environments. Technical personnel work in partnership with other AT&T service and service delivery organizations and divisions to evaluate threats, determine protective measures, create response capabilities, and assess compliance with best security practices, AT&T's Security Policies and Requirements (ASPR), and Networx contract requirements.
- **Corporate Security** – Provides support for physical security, protection of proprietary information, theft, fraud, and Code of Conduct violations.

- **Business Continuity and Security Services** – Provides Networx site and/or service specific disaster recovery and business continuity support for manmade or natural disaster events..
- **AT&T Global Security** – Provides logical and cyber security support for computing and networking outside the domestic US.
- **AT&T Labs** is AT&T's research and development organization that provides innovative network security products and technical solutions.

Security management personnel assigned to Networx are well versed in the use of current security technologies, and they hold recognized industry certifications such as Certified Information System Security Professional (CISSP) and Certified Information Security Manager (CISM). They also hold vendor-specific security certifications from Cisco, Microsoft, and others.

Figure 6.1-1: The security manager within the CSO organization. *The security manager functionally supports the Contractor Program Organization for all of AT&T's Networx customers.*

AT&T's security management will utilize these AT&T human resources in support of Agencies' task orders under Networx. Many of the staff members have obtained Government security clearances specific to the task order that they support, including Top Secret with sensitive compartmented investigations and life-style polygraph. Currently, approximately [redacted] AT&T personnel have clearances.

Networx security is managed in the CPO by the Networx Security Manager. The Networx Security Manager, a key staff member, manages the security of AT&T provided Networx services and the data associated with them according to the GSA's and Agencies' requirements as described in the proposal. The Security Manager is also responsible for the delivery of the required monthly and incident reports, updated Security Plans, and Risk Assessment reports to the GSA and appropriate Agencies. Within the Networx Contractor's Program Organization (CPO) as illustrated in **Figure 6.1-1**, the Security Manager has the support from the other functional areas and has the authority to acquire information from these support teams as may be required for specific investigations, tasks, or emergencies.

6.2 Security Management Practices and Procedures

As part of standard security management practices and procedures, AT&T utilizes the Federal Government and industry standard generally accepted security principles and practices to protect the confidentiality, integrity, and availability of information created, processed, transmitted, or stored by or for the Federal Government. AT&T's security management process employs a variety of teams specializing in various security disciplines, utilizing these

teams to enhance the overall knowledge base, ensuring that all aspects of security management are being considered.

Although the Agency's designated security management team is responsible for performing most daily system security administration, customers generally contract with AT&T to assume significant security management responsibility, which include one or more of the following:

- Review and assess requests for changes in security configurations
- Design secure solutions
- Plan and execute various security activities such as risk assessments and security test and evaluations
- Evaluate and install patches and updates as necessary
- Perform periodic vulnerability and network analyses
- Conduct security audits and assessments.

AT&T has multiple specialized teams available in both the managed and professional services areas to fulfill such responsibilities. All security activities are managed through the customer's designated security management team to employ consistent, industry accepted practices and to comply with the appropriate Federal guidelines and Networx contract requirements.

AT&T will identify the security management team responsible for maintaining an acceptable level of security during the system's life cycle. The security management responsibilities are described below.

Security Administration activities encompass creating or updating security policy and procedures to meet new or modified Government information security and assurance requirements; maintaining and updating a System Security Plan that outlines the controls and countermeasures to meet the Government security requirements; maintaining personnel security controls;

scheduling and performing periodic analyses; reviewing and authorizing changes in the security configurations, controls, or posture of the environment; and coordinating with other functional groups providing services to help protect the overall environment. Coordination often includes working with AT&T suppliers, vendors, and partners to help to deliver both IT products and services as expected and as required for network implementation and integration projects.

Operational assurance to assess whether, on an on-going basis, the system is operated in compliance with system security requirements. This includes monitoring both the actions of the people who operate the system and the functioning of the security controls, as well as conducting periodic risk assessments to maintain procedures consistent with security requirements and policy.

Security operations, which include routine operational tasks such as providing for scheduled backups and off-site storage of backup media; providing user security awareness and education; maintaining contingency and incident response plans and testing them annually; implementing risk mitigation measures identified through assessments or new developments in technology; and monitoring, testing, and installing operating system patches and upgrades.

Audits and monitoring, which include automated vulnerability assessments and the daily monitoring of intrusion detection system and firewall logs.

Incident response and reporting activities include detecting, investigating, and mitigating suspected or actual security violations or breaches of security policies and controls; notification and reporting of findings and mitigations strategies to management, and notification to the Government for determination of post-mitigation procedures such as prosecution.

6.3 AT&T Security Resources, Strategies, Policies, and Procedures

The ASPR Library is a series of documents establishing the security standards for protecting AT&T computing and networking infrastructure and is managed by AT&T's Security Center of Excellence. The ASPR documents do the following:

- Define specific security objectives
- Set a minimum baseline for securing the AT&T computing and networking infrastructure
- May be supplemented with more stringent requirements as determined by providers of service
- Are a mandatory component of AT&T's computing and networking development, management, and maintenance.

The ASPR documents describe the physical security and intellectual asset security managed by the Corporate Security organization. It is mandated within AT&T that employees follow these policies and put proper safeguards in place to protect AT&T's assets. The Corporate Security organization also oversees AT&T's Code of Conduct Program. The Code of Conduct provides information about the standards that AT&T expects all employees to follow, which are most clearly embodied in the values of AT&T's conduct awareness mission statement, "Our Common Bond" — respect for individuals, dedication to helping customers, highest standards of integrity, innovation, and teamwork.

This extensive body of knowledge and corporate culture meets or exceeds the spirit and intent of all relevant portions of FISMA, OMB, NIST, and FIPS Standards and Guidelines, and is applicable to all service elements, systems,

applications, workstations and support staff employed to provide AT&T Networx services.

6.4 AT&T Security Best Practices

Customer Agencies that procure AT&T's Networx services will benefit from AT&T's consistent approach to basic service security. This approach involves establishing basic goals such as:

- Maintain the availability of services
- Safeguard the integrity of the networks and support systems as well as the information available on the networks and stored in the support systems
- Preserve the confidentiality of information available on the networks and stored in the support systems
- Prevent the fraudulent use of the services

AT&T's approach to accomplishing these basic goals includes the following strategies:

- Taking a leadership role in research and development and participating in organizations and forums to elicit common strategies and priorities
- Assigning experienced networking professionals to monitor, analyze, and implement security solutions
- Managing and developing security solutions to Service Level Agreements
- Maintaining 24x7 Global Customer (GSA and Agencies) Support
- Offering customized and managed solutions for specific requirements

The most effective service security designs and implementations must be continuously managed and analyzed for improvement, as illustrated in **Figure 6.4-1**. AT&T views service security as a process driven by management and user awareness and supported by expert skills and advanced technology.

Figure 6.4-1: AT&T's Continuous Process. *AT&T will continuously analyze and assess Customer Agency assets to apply best security practices.*

Security controls will be designed to protect Government and AT&T information, resources, and systems from fraudulent usage, unauthorized access, and service disruption. Planned protections include segregating each Agency's data. The Customer Agency will know how their services are protected as well as what processes will be engaged in the event of a security issue.

AT&T has exacting security requirements that apply to our suppliers, vendors, and partners. Suppliers, vendors, and partners must adhere to ASPR and Networx contract requirements to secure AT&T networks, systems, and the data stored or traveling through the infrastructure that support Networx services, Networx OSS, and databases.

The relationships that are established with the suppliers are contractually managed by AT&T's Supplier Management Division (SMD). AT&T's Networx Security Manager will work with SMD and the Networx Business Manager in the CPO, to establish the GSA's and Customer Agency's requirements for delivering Networx services with AT&T's suppliers. AT&T uses the same management

methods and organizational interface processes regardless of whether it is a supplier, vendor, or partner.

The AT&T Networx Security Manager will work with suppliers, vendors, and partners to verify that inter-company interfaces meet AT&T defined processes and operational metrics are consistent with Networx requirements. These inter-company interfaces and processes define supplier, vendor, or partner security contacts and the escalation and remediation procedures to be followed in a fault situation. These procedures are documented and agreed to by the supplier, vendor, or partner to faclitate clear communications and expectations.

The AT&T Security Manager meets with the Networx Program Manager and/or Security Manger for each of our suppliers, vendors, and partners once a quarter to review all metrics and discuss how to improve operations methods. AT&T performs an annual test of procedures to ensure ongoing and verifiable quality assurance. If a security issue should arise, more frequent meetings would be conducted.

Requirements for product-specific security plans, quarterly operations reviews, and escalation and remediation procedures are included in each agreement with our supplier, vendor or partner.

AT&T's security management organization has built extensive relationships with the major network component providers, often receiving advanced notice of security issues prior to public release. AT&T has developed a complex security notification and patch management distribution application that has received industry accolades and is recognized as a proactive step in identifying network anomalies and worms before their destructive impacts are noticed. This system provides advanced notice for network administrators to take preemptive action to minimize network outages. AT&T hosts annual security seminars where customers, suppliers, and partners are invited to discuss the latest security prevention measures, latest trends and technologies available for deployment.

6.5 Employee Security Awareness and Training

AT&T has an extensive employee training and awareness program that includes annual Code of Conduct review and the Corporate/Personal Integrity Program (C/PIP). By AT&T's corporate policy, anyone performing work on behalf of AT&T and its customers must comply with the ASPR, thereby additionally securing Networx information and assets from unauthorized access, interception, disclosure, misuse, modification, destruction, theft, or impairment. This same level of protection for information and assets is required when working from non-AT&T locations.

This accountability is documented and communicated through Company security policies and the AT&T Code of Conduct. It is also documented and communicated to non-AT&T employees through the appropriate legal documents used to establish a business relationship with the Company. Such legal documents may include memorandums of understanding,

contracts, nondisclosure agreements, and agreements regarding intellectual property. Code of Conduct training is conducted yearly with all employees. Non-AT&T employees who sign the appropriate legal documents, such as nondisclosure agreements, are updated on a regular basis as required by the signed agreement.

AT&T individuals who will perform specific security roles for a Networx system (e.g., system administrator, security administrator, database administrator) will undergo specialized training focused on their respective role. Prior to being granted system access, all AT&T and AT&T subcontractor personnel working on a Networx service will read and maintain awareness of the information contained in the security plan.

6.6 Security Risk Management

AT&T employs several hundred security professionals to support risk management throughout AT&T services and support systems. As part of the process, AT&T uses a comprehensive set of company-designed and commercial tools and technologies to detect, prevent, analyze, and respond to security vulnerabilities and attacks. The work is organized into five areas,

each containing several programs dedicated to providing computer and networking security support. **Table 6.6-1** lists these five areas and the supporting programs, starting with security policy, which is the basis for the security risk management activities throughout the other four areas.

SECURITY POLICY AND REQUIREMENTS	PERIMETER/NETWORK/ SYSTEM PROTECTION	INCIDENT RESPONSE	VULNERABILITY DISCOVERY AND CORRECTION	RISK MANAGEMENT
General Security Policies	Firewall Management	Alert Processing	Network Scanning	Security Analysis
Specific network and computing requirements	Anti-Virus Management	Incident Reporting	Network Architecture Reviews	Escalation Procedures
Policy Exception Management	SPAM Management	Incident Response Program	Service Delivery Reviews	Threat Management
Risk Agreement Management	Intrusion Detection	Intelligence	Development and Testing Reviews	
Policy Communication and Awareness	Deception Technology (Honeypots)		Database Scanning	
	Secure Communications		Application Scanning	
	ID/Token Administration		Host Scanning	
			Enforcement Policy	
			Logical Assessments	
			AT&T Policy Compliance Management	

Table 6.6-1: AT&T Network Security Programs. *AT&T uses a comprehensive array of service and support system security programs to manage security risk to all the Networx services.*

The following sections describe major components of AT&T's risk management program, including vulnerability assessment, risk assessment, security management, and incident response.

6.6.1 Vulnerability Scans and Tests

AT&T will include as part of the yearly security risk assessment, a security vulnerability review of all Networx OSS as they pertain to confidentiality of the OSS and Government information that may be stored and made available by

the OSS. In addition to the yearly security risk analysis, monthly vulnerability scans are performed on all OSS. This includes the Networx OSS and the Networx Portal. Vulnerability scanning consists of system-level tests for security policy compliance and system configuration. AT&T conducts monthly network and host scans of internally and externally exposed systems and network elements using Commercial Off The Shelf network scanners which are in support of the Security Risk Assessment guidelines of NIST SP 800-30 and routine security verification.

6.6.2 Security Evaluation Program

AT&T's Security Evaluation Program (SEP) identifies and documents network security procedures that support ASPR and the Networx contract requirements to mitigate risks to AT&T's networking environment. This program is designed to evaluate the security of both existing environments and the security for new features that are delivered. It also allows AT&T to embed security in the lifecycle process for all AT&T services.

The SEP process identifies vulnerabilities through assessments, consultations, and/or security tools such as network/database host scanning tools. All identified vulnerabilities are categorized and entered into AT&T's vulnerability tracking system. Priorities for resolution are set based on the vulnerability classification assigned. Identified vulnerabilities are monitored and tracked to their ultimate resolution by an assigned AT&T security specialist. The Vulnerability Discovery and Correction tasks listed previously in **Table 6.6-1** outline the process, which includes compliance review, through the SEP.

Risk assessment is an on-going part of security risk management. AT&T will use the NIST SP 800-30 methodology to conduct risk assessments annually for all systems under Networx.

Risk assessments are initiated early in the system development life cycle. Security risks are identified and documented, and mitigating steps identified and included in the POA&M document. The AT&T team will track POA&M items to closure as part of on-going information assurance life-cycle management.

AT&T will work with Networx system owners to update existing risk assessments annually. As part of the risk assessment process, AT&T will assess all aspects of information security, including physical, personnel, operational, administrative, and telecommunications, making all commercially reasonable efforts to identify all security risks, regardless of their severity. Annually AT&T will prepare a Security Risk Assessment Report describing the results of each assessment and submit it to the Government for approval. The report will describe threats, security vulnerabilities identified and their associated risks, likelihood that the risks will occur, impact of the risks to the Government, severity of the risks, mitigation strategy, and commercially reasonable measures that AT&T recommends to mitigate the risks. The report will include an analysis of security vulnerabilities of all Networx Services, Networx OSS, and databases as they pertain to the

confidentiality, integrity, and availability of the services and Government information created, processed, transmitted, or stored by the environment. The risk severity will be categorized based on the potential impact that the security risk may have on the Government, as defined by the "Potential Impact" categorization described in FIPS PUB 199 guidance.

The AT&T risk mitigation strategy for reducing or eliminating the vulnerabilities found during the risk assessment will be documented and submitted to the Government for discussion, review, and approval. The Security Risk Assessment Report will include an estimated timeframe needed to implement additional security controls.

The methodology for the risk analysis is based on NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*. There are nine steps defined in this document for the risk analysis process.

1. **System characterization:** The scope of the effort is defined by gathering system related information such as hardware, software, system interfaces, system criticality and sensitivity. Information regarding the system is gathered in various methods such as interviews, documentation reviews, questionnaires, and automated scanning tools. The result of the system characterization is the identification of the system boundary and scope.
2. **Threat identification:** All potential threats and threat sources that could exploit system vulnerabilities are identified.
3. **Vulnerability identification:** All system vulnerabilities that could be exploited by the potential threat sources are identified. Various methods could be used for identifying system vulnerabilities such as system security testing or development of a security checklist.
4. **Risk analysis process:** The security controls that are planned or in place are analyzed in order to minimize or eliminate the risk of a threat source exploiting system vulnerability.

5. **Likelihood determination:** An overall likelihood rating of the threats that may exploit identified system vulnerabilities are derived. The likelihood ratings are based on the threat motivation, nature of the vulnerability, and the effectiveness of the security controls that are in place.
6. **Impact analysis:** The adverse impact of a threat exploiting a vulnerability is determined. The adverse impact of a security event can be described in terms of loss or degradation of integrity, availability, and/or confidentiality. The result of this step is a magnitude of impact rating expressed as high, medium, or low.
7. **Risk determination:** The risk level of the system is determined. The risk level is derived by multiplying the likelihood and the magnitude of impact ratings.
8. **Control recommendations:** Controls that could mitigate or eliminate the identified risks are presented. The goal of these recommended controls is to reduce the level of risk to the system to an acceptable level.
9. **Results documentation:** Results must be documented in the risk assessment report. The Risk assessment report must clearly describe the threats and vulnerabilities, measure the risk, and provide recommendations for control implementation

AT&T will work with Networx system owners to evaluate the impact of any additional security controls that the Government determines are required. The evaluation process will identify security risks associated with implementing these controls and identify steps to mitigate the security risks to Networx services and the OSSs consistent with the Federal Government accepted security principles and practices per NIST Special Publication 800-14. AT&T will track the newly implemented controls and countermeasures and work with the Government to provide evidence the required mitigation strategies are in place and documented.

AT&T will assess and include as part of the yearly security risk analysis security vulnerabilities of all Networx OSS as they pertain to the confidentiality of the OSS and Government information that may be stored and made available by the OSS. AT&T performs application and database vulnerability scanning. This application and database vulnerability scanning uses Commercially Available Off the Shelf tools that are specifically configured to scan Networx OSS and Networx Portal applications and is a key component of security risk mitigation. The application vulnerability scanning simulates web application attacks, points to potential security loopholes and provides guidance and advice on how to remediate any bugs discovered and is based on four stages of operations:

- **Crawl -** dynamically crawls through the scanned site unassisted, discovers the links, and recognizes the application security policy.
- **Analysis –**identifies known/unknown vulnerabilities specific to the site, such as hidden manipulation or cross-site scripting. After identifying the vulnerabilities, the application vulnerability scanner creates mutated links that will be used in the Attack stage to test the site. The knowledge database inside the scanner contains a continuously updated list of vulnerabilities and hacking techniques.
- **Attack** – the scanner sends the mutated requests to the site and ranks the attack results by severity and success rating.
- **Reporting** – the scanner generates reports customized with recommendations for the remediation of each vulnerability.

The database vulnerability scanning performs three categories of security checks.

- **Authentication checks** – verify all settings for each user's claimed identity within the database management system including password strength analysis, password aging, login attacks, stale logins, default login and passwords checks, and security of administrative accounts.

- **Authorization checks** – focus on how an authenticated user is permitted to use specific resources within the system which includes account and role permissions, stored procedures access, unauthorized object owners, resource access and permissions.
- **System Integrity checks** – focus on the coordination and control of system resources within the system which includes Trojan horses, operating system integrity, audit configuration and analysis, buffer overflow vulnerabilities.

6.7 Information Security Management

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. AT&T will deploy boundary protection devices, such as firewalls and intrusion detection systems, as required. AT&T will monitor deployed devices in compliance with ASPR and the Networx contract requirements. Additionally, AT&T will monitor that personnel accessing Networx services are authorized and have the appropriate security clearance, in accordance with the customer Agency's personnel policies.

AT&T will support and maintain the security guidelines adopted by the customer Agency. In addition to the guidelines, AT&T will support the Government in their efforts to comply with any statutory or regulatory requirements for the operation of a client Agency's task order.

A Networx system located onsite at the Agency or at AT&T will maintain the minimum set of required controls as specified in NIST SP 800-53, Annex 1, to protect the information pertinent to the secure operations of the Networx system. The security controls deployed will promote the confidentiality, integrity and availability of Networx data at the Government Agency and AT&T premises. AT&T will work with Networx system owners and make available approved encryption technologies to support confidentiality and integrity requirements of Government generated information.

In order to promote data confidentiality and protection from unauthorized disclosure, AT&T will implement personnel identification and authentication services. AT&T or Government personnel may be granted privileged system

access if required for a legitimate job function. Such users will be responsible for operating and managing Networx services in accordance with NIST SP 800-14 guidelines.

AT&T will use various security controls to protect Networx infrastructure and assets from unauthorized access attempts. These controls include the use of firewalls, Intrusion Detections Systems, packet-filtering routers, and Access Control Lists (ACLs) implemented on boundary routers.

6.8 Information Assurance Management

AT&T's Information Assurance (IA) security principles and practices adhere to Federal Government accepted practices for protecting system databases, OSS, and information processing systems that are critical for the continuous, reliable operation of Networx systems

AT&T provides access controls to protect its OSS and switching systems from attacks via publicly accessible ports, such as maintenance ports. Protection mechanisms are consistent with Federal Government accepted security principles and practices per NIST Special Publication 800-14 guidance. These access controls restrict access to network management or customer-related information to authorized contractor and Government personnel only. AT&T also adheres to these principles and practices to protect its transmission facilities, switching components, network management systems and other essential facilities from denial-of-service attacks, intrusions, and other perceived threats.

AT&T ensures protections are implemented to secure Networx databases, OSS, and information systems managed, maintained, and/or hosted by AT&T.

AT&T will provide evidence that security controls for Networx services and Networx OSS as specified in the security plan are implemented correctly, operating as intended, and producing the desired outcomes in meeting Government security requirements. Such evidence includes security test results, evaluations, and audit findings that have been captured and documented within the previous 12 months.

AT&T will provide the Security Plan including a Risk Assessment within 30 days of Notice to Proceed and updated annually within 30 days after the end of each contract year.

6.9 Security Breach Response Management

In accordance with FISMA and OMB Circular A-130 Appendix III, AT&T will provide an incident response capability for systems contracted under the Networx program to respond to and manage security breaches. A security breach or 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 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, OSS, and databases by protecting them in a

security enclave bounded by firewalls and IDSs. IDSs are used to monitor network traffic for potential misuse or policy violations.

AT&T will provide an Incident Response Plan as a component of the Security Plan in accordance with NIST SP 800-18 within 30 days of Notice to Proceed, updated annually within 30 days after the end of each contract year. The Incident Response component of the Security Plan will describe in detail the incident response procedures to be implemented in the event that a security breach occurs. The plan will include the following:

- The requirements for incident response handling
- Objectives for incident response handling
- The 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.

AT&T will implement controls as appropriate to identify and correct security-related system and network vulnerabilities. Upon request, AT&T will advise agencies on 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.

In the event an incident, suspicious activity, or security breach is detected, AT&T will notify the Government in accordance with Networx requirements.

6.10 Alarms and Audit Trails

Security monitors, intrusion detection systems, and other security management capabilities implemented by AT&T as appropriate for Networx systems, networks, and services will utilize various alarms to alert security personnel responsible for monitoring systems. AT&T also will log Networx OSS and private Networx website security violations and other security related-events and transactions. See Section 5.3, Audit Trails, for additional details.

Logs will be secured, reviewed, and archived in accordance with the Federal Acquisition Regulation (FAR) Subpart 4.7. AT&T will provide logs of security violations, transactions, security-related events, alarms, and associated electronic reports to the PMO as required by FAR Subpart 4.7 at no additional cost to the Government.. Also, if the PMO requests, AT&T will maintain audit trails longer (for a maximum of three additional years) or turn them over to the PMO via electronic medium upon written request.

Within 60 calendar days after Notice to Proceed, AT&T will propose a process to maintain real-time operational procedures and capability for detecting and monitoring suspected abuse or intrusions to the network for those events that require immediate attention by PMO, affected Agency or site, and/or contractor staff. AT&T and the appropriate party will review the process and determine if any changes need to be made prior to implementation. Further, AT&T will update the process and procedures requested by the Government as appropriate.

6.11 Personnel Security

AT&T has extensive experience initiating background investigations of personnel requiring national Agency checks and will initiate those requests as identified by the Government. The AT&T security office currently initiates and processes an average of 56 new security clearances each month. Upon award and as requested by the Government, AT&T will obtain and maintain all appropriate personnel and facility clearances to have access to and custody of such information, up to and including Top Secret as required at no additional cost to the Government. AT&T will take actions to allow the proper paperwork to be received for processing within 30 days, according to OPM instructions. See Section 4.1, Personnel Security, for details.

AT&T will obtain information about Top Secret and other security clearances from the following organization:

Center for Federal Investigative Services
U.S. Office of Personnel Management (OPM)
1900 E Street NW, Washington, DC 20415-1000
(202) 606-1800
TTY (202) 606-2532

6.12 Physical Security

AT&T will follow Federal Government generally accepted security principles and practices per NIST SP 800-14 to provide Networx physical security. AT&T will make every reasonable effort to safeguard Networx services-related facilities and equipment against sabotage, espionage, damage, and theft consistent with the criticality of the facility or equipment to the Networx Program. AT&T will make every reasonable effort to 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 processes, stores, or transmits Networx-related information or data.

AT&T will 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 criticality of the work being performed or the sensitive nature of the Government information being handled. Electronic and physical methods of security include guards, intrusion detection devices, surveillance cameras, lighting, and fencing. See Section 4.2, Physical and Environmental Protection, for details.

AT&T will make every reasonable effort to protect its Networx services operations facilities from basic service interruptions such as those caused by electrical outages or flooding and will protect its Networx services operations facilities by meeting fire code regulations specific to the location of the facility. AT&T will make every reasonable effort to 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.

As part of its NIST-compliant contingency plan, AT&T will provide offsite backup and storage of critical Networx services configuration and OSS data and information generated and stored at its Networx facilities in accordance with the Networx Contingency Plan. Critical data and information is any data or information that is essential for the restoration of services and operation in the event of a disaster that impacts the contractor's Networx facilities or operation. Near real-time mirrored storage is used for all databases. The storage servers are located at offsite locations.

6.13 Security Refreshment

The Security Risk Assessment will be updated annually, within six months of a major system upgrade, or as new threats and vulnerabilities are identified and mitigation controls and countermeasures are implemented. The effectiveness of security controls is reviewed and assessed through the Security Test and Evaluation (ST&E), vulnerability scans, and security self assessments. AT&T will provide summaries of security-related events and will work with the Government on an ongoing basis to determine the severity of new threats and to enhance the security controls. The self assessment will be performed annually on systems supporting Networx services, Networx OSS, databases and the **Business**Direct® portal, in accordance with NIST 800-26 with the Security Risk Assessment to be updated accordingly and provided to the Government. AT&T will help to enable

the security of the system by applying appropriate patches for all known vulnerabilities in accordance with AT&T patch management policy.

AT&T employs the same process on all of the OSS and service components software. System administrators (and their back-ups) are immediately notified about any vendor developed or AT&T internally developed patch via an email notification system. The system administrator first verifies that the patch will not cause system or application instability. After this is verified, the patch is applied by the end of the same day as the receipt of notification and/or verification. In the event that patches may cause system or application instability, the specific identified security vulnerability is mitigated using a combination of firewall rules, intrusion detection system signatures, and network and system packet filters to protect the un-patched systems until the patches are successfully applied.

Re-evaluation and continuous improvement are institutionalized within AT&T through a combination of expert councils and trend analysis. The AT&T security organization maintains a Security Business Controls Council comprised of the managers who lead our major security programs and core functions. One of the primary goals of this council is to periodically review security objectives and technology to ensure policies, programs, and resource allocations are commensurate with current and changing threats.

AT&T also gains insight into emerging trends or threats through active participation in many 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) certification. 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 a training program by taking classes either on-line or in -person.

AT&T will use a combination of commercial and proprietary information security applications to maintain and secure Networx services, Networx OSSs, and databases. This comprehensive approach to data security involves deploying:

- Two factor authentication
- Encryption and VPN
- Firewalls
- Host and network based intrusion prevention
- Network monitoring
- Scanning and vulnerability detection
- Redundancy

AT&T will take an aggressive approach in anomaly detection to prevent the spread of malware and software robots (“bots”). AT&T will also evaluate the use of new technologies in the wireless, RFID, and biometrics arena in order to expand the list of security solutions available to Networx participants. AT&T will also maintain 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 of the vulnerability will give AT&T time to prepare mitigation strategy. AT&T will also participate in vendor forums and workshops and will keep our 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.

6.14 Non-Domestic Services Security Management

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 the best commercial security practices in supporting service delivery to non-domestic locations.

AT&T will monitor the performance of its foreign subcontractors' business partners and Post Telephone and Telegraph (PTTs) operating administrations' services and immediately report verbally to the PMO and the Contracting Officer (CO) any unusual or suspicious outage, blockage, or tampering that may indicate that users of services are being denied service or are being compromised. AT&T will notify the PMO and impacted Agencies of unusual or suspicious outage or activity and will make written notification within 7 days of suspected event.

AT&T monitors the quality of the connections between the the PTTs at the AT&T network Interface as well as from network management information from the Premise Edge equipment. The monitoring methods used will be described in the updated Security Plan which will be updated to reflect current methods employed to identify suspicious outages, blockages, or tampering that indicate that service is being denied or compromised.

6.15 Fraud Prevention Management

AT&T's approach to fraud prevention is to incorporate adequate security controls to help to prevent, detect, and report fraudulent use of services and security breaches for its network, OSS and databases used for the Networx program. The approach focuses on two distinct areas of the comprehensive end-to-end AT&T Security process: applied research on security threats to appropriate network traffic behavior and algorithms and tool development/deployment for operations use.

On a weekly basis throughout the year, the AT&T Labs scientists and SCOE engineers meet to review and evaluate emerging threats and prioritize the features required for new software within the AT&T's network monitoring systems. This information is then used to task AT&T Research scientists who, working with AT&T's Security Center of Excellence (SCOE) engineers, are assigned to analyze, characterize and develop algorithms that detect anomalous events within AT&T's network.

AT&T proactively adapts to new network threats by directly linking a research staff engaged with exploring emerging security threats to an engineering/operations organization responsible for AT&T's worldwide security management. 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. These tools include:

1) Advanced computer systems using customized processes to detect protocol and port activity deviations from expected values for every hour of every day

2) Algorithms written specifically to detect traffic patterns that match those of a propagating worm or host scanning operations

3) Use of tools for internal "white hat" security scanning

4) An extensive knowledge base built from years of security incident case information

5) Established processes supported by pre-defined procedures, contact lists, bridge numbers and warning letter templates as well as best practices for conducting a thorough investigation and criteria for escalating to additional layers of support.

As an example of our fraud prevention procedures, we describe here our calling card fraud prevention program. AT&T has a comprehensive calling card fraud prevention system to handle millions of cards distributed globally on an annual basis. Below are some examples of fraud controls AT&T has in place:

- **Account passwords** provide an extra measure of protection against unauthorized and fraudulent use of the calling card and administration of the Card Account Detail.
- **Card Security Specialists** advise users in the prevention of fraud on the calling cards.
- **Control of multiple attempts** establishes a threshold limiting simultaneous use of a single card so multiple call attempts are controlled in real-time.
- **Fraud protection** provides threshold monitoring of card usage to detect unusual calling patterns. AT&T disconnects lost or stolen calling cards immediately (within 15 minutes) after receiving a report of a compromised card (including lost or stolen cards).
- **Randomly-generated card numbers** instead of easily-abused customer business or home phone numbers makes the job of a potential unauthorized use much more unlikely.
- **Suppressed PIN option** prevents an unauthorized person from observing the entire card number while the cardholder is making calls. This option consists of not printing the Personal Identification Number (PIN) or the last 4-digits on the card. Without the entire card number, including the PIN, calls cannot be made.
- **Terminating Code Screening** (TCS), available to AT&T calling card customers, blocks calls from certain locations to specific countries or areas or vice versa. For example, in the USA, locations are usually public phones

subjected to high international telephone fraud. It is possible to override the TCS block on cards that have a legitimate need for calling card capabilities from/to blocked countries.

- **Terminating Code Screening (TCS) Override** provides the ability to overcome the TCS restrictions. The customer can call the closest AT&T Customer Care Center, where the service representative asks for customer identification and sends out a form that the customer fills out and faxes back. The AT&T Customer Care Center then makes the necessary arrangements with the AT&T Card Protection Center, which permanently overrides the TCS blockage on a card-by-card basis. TCS Override allows legitimate calls to be placed by cardholders with a need to reach those areas.

AT&T's wireless partner provider for Networx, Cingular, has a fraud protection program to prevent fraudulent use of wireless services. Fraud protection program controls include the following:

- **Authentication**, which involves the exchange of secret codes based on a complex algorithm between the phone and the switch.
- **Fraud Management System (FMS)**, a computerized "burglar" alarm system for identifying cloned phones and subscription fraud. When a subscriber's usage deviates from its normal activity, it trips an alarm in FMS. A fraud analyst will investigate and ascertain the legitimacy of new services or whether a customer has been victimized and remedy the situation.
- **Pre-Call Validation** – The Subscriber Identity Module, commonly known as a SIM chip, is critical to the pre-validation process for GSM based networks. The SIM chip that is issued for each GSM subscriber is actually a micro-computer. Specific to the pre-validation process, the SIM chip contains a code that is automated and only the network can read (users don't have access to view or modify the code). Once the mobile handset is

turned on, the user is identified and authenticated as the SIM chip communicates through the handset with the network. The GSM network verifies the user by sending it a challenge. The data in the challenge is then processed via a non-published proprietary GSM algorithm. The handset together with the SIM chip computes a response to the challenge and sends it to the GSM Network. The GSM Network performs a similar computation and then compares the subscriber's answer to the locally generated answer. If the answers match, the user is authenticated and allowed to use the network. Service can be blocked if the user's equipment or SIM chip has been reported lost or stolen. Under such circumstances SIM chips will fail this initial authentication process and will not be granted access to network services.

- **Roaming Authorization per MSC (RAM)** enables a fraud analyst to suspend roaming privileges in any market(s) for a specified length of time where fraudulent activity is suspected. As a result, the counterfeiter will be denied service in those markets, while the valid customer continues to have use of their phone at home and in all other roaming markets. (Note: Under Federal law, access to wireless 911 is never restricted).
- **Fraud Awareness Training** is provided for each and every employee of Team partner Cingular Wireless. This training educates employees on the magnitude of the problem, the various types of fraud, how fraud is committed, and how it is being fought. The training also teaches employees how to identify and handle a fraudulent situation.

In the event fraudulent use of services is detected or suspected, AT&T will notify the Government in accordance with Networx contract requirements.

A key concept in detecting fraud is first determining what is considered "normal" activity. AT&T will use a combination of commercial and proprietary applications to ensure Networx information is not exploited and misused.

This proprietary software both analyzes information packets and performs trend analysis on all data traversing AT&T networks using techniques developed and refined at the AT&T Labs. AT&T Fraud experts will also stay current with the latest advancements in fraud prevention and detection by attending the latest Fraud Prevention seminars and conferences. In compliance to Corporate Policy, AT&T maintains and reviews system activity logs for improper use on a regular basis. AT&T will also notify the appropriate Networx contacts once abnormal activities have been detected. AT&T maintains a close relationship with law enforcement officials and will fully cooperate with any investigations into suspicious activity or use.

6.16 Future Security-Related Technologies

AT&T security management will work with Government PMOs to address the information security implications of emerging information technologies. First, AT&T will assist the Government in assessing whether new technologies are appropriate in the Networx environment, from an information assurance point of view. As new and emerging technologies, such as wireless LANs (Wi-Fi), are introduced into the Networx environments, for example, AT&T will work with the Government to research, analyze and evaluate these technologies to minimize any additional risk or vulnerabilities into the Networx environments.

AT&T will help to ensure new, proven technologies are applied in a practical and methodical manner that will enhance the security posture of the Networx environments. Examples may include strong user authentication technologies, such as biometrics, RFID, and encryption technologies.

AT&T will work with the Government to develop new security requirements and to satisfy current NIST and Federal Government mandated configurations in association with the implementation of new technologies.

ATTACHMENT A:
RULES OF BEHAVIOR

INTRODUCTION

In support of individual client Agency task orders, this document describes the general rules of behavior to be followed by all users of Government systems computing resources to support the mission and functions of the Government. The intent of the computer system user IT security general rules of behavior (ROB) is to summarize laws and guidelines from various Federal laws and regulations, most specifically OMB Circular A-130, for the use of computing resources.

What are "Rules of Behavior (ROB)"?

The ROB are part of a comprehensive program to provide complete information security. ROB establish standards of actions in recognition of the fact that knowledgeable users are the foundation of a successful security program. The ROB concern use of, security in and the acceptable level of risk for Government computer systems, and highlight the need for users to understand that taking personal responsibility for the security of a computer and the data it contains is an essential part of their job. People are the first line of defense in support of information and information systems. Users offer many eyes and ears to detect and report threats to information systems.

Who is covered by these rules?

These rules apply to everyone under a Networx contract who is using Government computing resources or accessing Government systems under formally established agreements. All users should be fully aware of, and abide by the security policies as well as related Federal policy contained in Privacy Act and the Freedom of Information Act. All users will review and provide signature or electronic verification to these rules annually.

What are the penalties for Noncompliance?

Compliance with these rules will be enforced through sanctions commensurate with the level of infraction. Actions may include a verbal or

written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation. In addition, activities that lead to or cause the disclosure of classified information may result in criminal prosecution under the U.S. Code, Title 18, Section 798, and other applicable statutes.

Responsibilities

Complying Users will:

1. Process, store, and/or transmit classified data only on systems and/or networks authorized for the highest level of the classified data involved.
2. Protect and safeguard information including media that contains information from unauthorized access, unauthorized or inadvertent modification, disclosure, destruction, denial of service, or use in accordance with applicable Department policy, practices, and procedures.
3. Protect all hard copy produced at the highest classification or sensitivity level of that system until reviewed for proper classification or sensitivity and control.
4. Destroy information or media, when required, in accordance with security requirements based on the level of classification or sensitivity.
5. Provide access to classified or sensitive information only after ensuring that the parties have the proper clearance, authorization and need-to-know.
6. Operate the computer only in those areas approved for the highest classification or sensitivity level of the information involved unless specific authorization has been received from the Information System Security Officer to operate the computer in other areas.
7. Store the computer in an approved security container (or in a facility approved for open storage) when it is not in use.

8. Never remove the computer (or hard drive) from authorized or cleared Government facilities without specific approval of the Information System Security Officer (ISSO).
9. Comply with terms of software licenses and only use Government -licensed and authorized software.
10. Use Government systems for lawful, official use, and authorized purposes in accordance with current guidelines.
11. Use the e-mail system in accordance with Government guidelines.
12. Not generate or send offensive or inappropriate e-mail messages, images, or sound files. Limit distribution of e-mail to only those who need to receive it.
13. Choose and change passwords in accordance with the Government security standards.
14. Not share account passwords with anyone.
15. Protect passwords at the highest classification and data sensitivity level of information on that system.
16. Know the system data and properly classify and protect all data inputs and outputs according to their sensitivity and value.
17. Properly mark and label sensitive and classified documents and media in accordance with the Security Program operations manual.
18. Remove sensitive information from hard disks that are sent out for maintenance. For classified data, consult with the appropriate ISSO and refer to the Security program operations manual for sanitization procedures for hard drives.
19. Screen-lock the computer or log off when leaving the work area, and power down the computer when departing for the day.
20. Use authorized virus-scanning software on the workstation or PC. Know the source before using diskettes or downloading files.

21. Not use shared drives to store, maintain, or relay Privacy Act data unless the data is password protected and the folder within the shared drive has access set up only for those employees authorized to work with the data.
22. Complete an annual IT security awareness refresher course offered by the Government Agency.
23. Sign all logs, forms, and receipts as required for accomplishment of duties relating to the collection, use, transfer, or disposal of information or information systems.
24. Know who their ISSO is for each computer system. Consult the appropriate ISSO and obtain permission or approval before doing any of the following:
    - Changing any configurations and/or settings of the operating system and security-related software on classified systems.
    - Installing any software.
    - Adding, modifying, or removing hardware accessories or networks to a classified computer.
    - Accessing the internal components of the computer.
    - Testing the capabilities of the security control software.
    - Circumventing the security mechanisms used on and by the computer.
    - Attempting to access any electronic audit trails that may exist on the computer unless specifically authorized to do so.
25. Make the computer available at any time to the ISSO for inspection and review of audit logs.
26. Make the computer available at any time to the System Administrator for the installation of patches and other system administration activities.
27. Report known or suspected incidents immediately. Immediately report to the ISSO any evidence of tampering with the computer or if the computer's tamper-evident seals are broken.

28. Notify the ISSO when access to the computer is no longer needed (e.g., transfer, termination, leave of absence, or for any period of extended non-use).
29. Never perform audit functions on a system for which the user is either a user or system administrator.

In addition to the above General Rules of Behavior, there are a set of rules for privileged users such as System administrators and mangers. Typical rules of behavior for privileged users are as follows:

System Administrators will:

1. Monitor whether the Certification Agent (CA) or a CA-appointed agent validates system security at least annually.
2. Make the computer(s) available for periodic reviews of the security configuration by independent testers.
3. Not serve as the system administrator and ISSO for the same system.

Managers will:

1. Provide staff with access to, and sufficient time to complete, the Security Awareness Training program or other annual IT security training offered by offices/bureaus/components.
2. Provide staff with access to, and awareness of, all existing policies and procedures relevant to the use of information technology resources.
3. Assess whether staff follows system security policies, guidelines and procedures

I acknowledge receipt of the General Rules of Behavior listing, understand my responsibilities, and will comply with the rules of behavior for Government systems.

_____ _____

Signature Date

Note: *Statement of acknowledgement can be provided via email.*

ATTACHMENT B:
RISK ASSESSMENT OUTLINE

RISK ASSESSMENT OUTLINE

1. SYSTEM CHARACTERIZATION

1.1 System-Related Information

1.2 Information Gathering Techniques

2. THREAT IDENTIFICATION

2.1 Threat-Source Identification

2.2 Motivation and Threat Actions

3. VULNERABILITY IDENTIFICATION

3.1 Vulnerability Sources

3.2 System Security Testing

3.3 Development of Security Requirements Checklist

4. CONTROL ANALYSIS

4.1 Control Methods

4.2 Control Categories

4.3 Control Analysis Technique

5. LIKELIHOOD DETERMINATION

6. IMPACT ANALYSIS

7. RISK DETERMINATION

7.1 Risk-Level Matrix

7.2 Description of Risk Level

8. CONTROL RECOMMENDATIONS

9. RESULTS DOCUMENTATION

10. RISK MITIGATION