

1.3.1 Approach to Ensure Infrastructure Security

[L.34.1.3.1]

Agencies are supported by continuous oversight and processes to provide a secure infrastructure designed to protect critical data on both physical and logical levels.

Network security is a cornerstone of AT&T's network philosophy. By following the security policy mandate of AT&T's Chief Executive Officer (CEO) as well as applicable regulations and legislation, AT&T protects its own information and resources and customers from unauthorized access, disclosure, corruption, or disruption of service. This security policy is applicable to AT&T network elements, systems, applications, and workstations owned or managed. Execution of this policy is led by the AT&T security organizations at the corporate and worldwide operational units. Security has ultimate responsibility for all aspects of network security. Specifically, security's role is to perform the following tasks:

- Own and manage security standards and guidelines
- Protect managed assets
- Supply security guidance and strategic direction to the business, worldwide security, and operations groups
- Provide consistent compliance globally to the network security program
- Implement and practice security standards
- Provide accountability of senior executives for security compliance in their business or region
- Coordinate a security review program to measure the degree of security compliance
- Maintain awareness of security industry changes and trends
- Develop and manage the corporation's global security education program

- Deliver security alerts and advisories to the corporate and worldwide service organizations
- Provide security specialist support to the operations and security teams
- Monitor and facilitate compliance with legal and regulatory security requirements.

AT&T's security policies and standards are based on the same criteria as International Organization for Standardization (ISO) 17799/British Standard (BS) 7799 standards. For security services, we implement the applicable Federal Information Processing Standard (FIPS) and National Institute of Standards and Technology (NIST) standards. In addition, security standards, operating procedures, tools, and other protective measures are reviewed regularly to verify that high standards of security are observed throughout the company.

As the Information Technology (IT) environment and IT security concerns change, AT&T is helping to mold the next iteration of standards. AT&T is an active member/leader/founder of several standards committees and consortia at the state, national, and international levels. AT&T approach security architecture is summarized in **Table 1.3.1-1**.

SECTION	SECTION DESCRIPTION
Section 1.3.1.a	Presents AT&T Protection Mechanism: Separation; Automation; Monitoring; Control; Testing; Response; Innovation
Section 1.3.1.b	Presents AT&T's measures to prevent cyber attacks <ul style="list-style-type: none"> • Follow Defined Network Management Techniques <ul style="list-style-type: none"> • Configuration Management • Enterprise Network Management • Automated Provisioning systems • Comprehensive Incident Detection and Response <ul style="list-style-type: none"> • Various system tools to detect and mitigate security risks
Section 1.3.1.c	Presents AT&T's approach to upholding best practices <ul style="list-style-type: none"> • AT&T is a leader in setting industry best practices • Security is designed into architecture of our network
Section 1.3.1.d	Presents AT&T's perspective on future security enhancements that will become available during Networx contract
Section 1.3.1.e	Presents AT&T's abilities to perform Certification and Accreditation (C&A) activities <ul style="list-style-type: none"> • Trained, experienced, and cleared personnel • AT&T C&A methodologies based on FIPS Publication 800-37

- Comprehensive C&A documentation and tools

Table 1.3.1-1: Response Summary for Section 1.3.1. Agencies acquire a comprehensive, proven security solution that provides protection for supported networks.

Securing the Government's network is a high priority to AT&T. AT&T has supported the Government in the past with securing their applications and will continue to provide security protection in the future.

1.3.1.a Security Mechanisms and Controls [L.34.1.3.1.a]

(a) Describe the mechanisms and controls that the offeror uses in its network(s) to ensure protection of the offeror's infrastructure and provide security for the services offered to its customers.

Agencies benefit from the mechanisms and controls AT&T uses in protecting our own network and providing worldwide network services to businesses in over 50 countries. The AT&T global network consists of multiple components which are converging into a single multiprotocol label switching (MPLS) Internet protocol (IP) network and transported over an intelligent optical core. These components include

To keep Agencies' traffic secure, service providers must secure their network infrastructure.

[REDACTED]
[REDACTED]
[REDACTED]

The IP network supports global Internet access services, IP MPLS-enabled virtual private network (VPN) services, and various services implemented in networked server complexes (e.g., voice over Internet protocol [VoIP], email/ domain name service [DNS], application hosting, network-based managed firewalls, and management of customer premises equipment [CPE]).

The key technological component in AT&T's current and future network evolution is MPLS. It is used throughout AT&T's global public IP network as well as its IP-enabled frame and ATM networks. AT&T has contributed significantly to its development and built years of experience with it. (Our first MPLS-based service was announced in 1999.)

At the network edge, AT&T has a rigorous set of security methods, processes, techniques, and practices (Table 1.3.1.a-1).

This is a necessary protection of the integrity and privacy of a VPN. A carrier must, however, also protect the service infrastructure against compromise or overload that might subvert the VPN.

AT&T's engineers maintain a constant security focus in all design, deployment, and operational processes around an MPLS core in seven protection areas: Separation, Automation, Monitoring, Control, Testing, Response, and Innovation¹.

AT&T SECURITY PROTECTION MECHANISMS AND CONTROLS

Separation

Customer traffic is separated using MPLS virtual private networks (VPNs).

CONTAINMENT

Traffic between customer-edge (CE) routers stays inside that customer's VPN – no spillover can occur based on adherence to RFC 2547. In addition, CE routers are private—they are physically separate from peered CE routers. This practice provides VPN user with protection from the Internet.

ISOLATION

No customer's VPN can, in any way, materially affect or influence the content or privacy of another customer's VPN, based on adherence to RFC 2547.

AVAILABILITY

No portion of AT&T's MPLS VPN service is peered with the Internet.

CENTER AND SERVICE COMPLEX PROTECTION

Network management centers, data centers, and service complexes are further protected by firewalls and intrusion detection systems—another example of domain separation.

SIMPLICITY

The simplicity and elegance of MPLS enhances security through improved provisioning, network management, and connectivity controls.

Automation

Automated perimeter security tools protect the MPLS core.

FILTERING

Automated provisioning and management of are used on all provider edge (PE) routers.

LEAST PRIVILEGE

are designed to restrict traffic only to connected CE routers for only required services.

LIMITS

is used to limit the number of transactions performed by a router.

is used to time out, limit, and lock out users after multiple access attempts.

Monitoring

IP traffic monitoring provides early warning of Internet viruses and worms.

ANOMALY DETECTION

Traffic is proactively monitored for evidence of worm and virus trends in real-

¹ To read a more complete discussion of this topic, refer to Appendix N, The Seven Pillars of Carrier Grade Security.

EXTERNAL ACCESS	time. Any external access to [REDACTED] is monitored on a 24x7 basis.
ANALYSIS	Statisticians continue to evolve algorithms for security anomaly detection.
	<i>Control</i>
	AT&T enforces strict operational security controls in its MPLS core.
PROCESSES	Well-developed methods and procedures are followed that are derived from decades of best practices in operating customer networks. Processes are routinely tested and validated for adherence.
CERTIFICATION	Operations are certified—wherever AT&T deems appropriate—to the best industry standards and are compliant with the National Reliability Industry Consortium (NRIC) certification requirements.
ROOT CAUSE ANALYSIS	Incidents are subject to comprehensive root cause analysis. This process is used to identify process improvements through any operational policy violations.
	<i>Testing</i>
	AT&T uses testing, audits, and reviews to ensure security compliance.
TESTING	Experts are constantly performing penetration testing on MPLS security controls.
AUDITING	Ongoing independent audits are used to confirm compliance with the security policy.
REVIEWS	All processes have embedded controls that require expert security reviews.
	<i>Response</i>
	AT&T deploys proactive response teams trained in the details of MPLS.
TIERED RESPONSE	Incidents are dealt with through a tiered response infrastructure that includes senior security and operations experts.
PROACTIVE INDICATORS	[REDACTED] acts routinely and proactively on indicators of any customer-visible problems.
NEW CUSTOMER SERVICE	This novel notification service extends 24x7 knowledge to customer-specific environments.
	<i>Innovation</i>
	AT&T funds extensive MPLS security research.
AT&T RESEARCHERS	AT&T researchers are exploring creative means to analyze anomalies, create algorithms for integrating control and data plane information, and use new means for MPLS management and monitoring.

Table 1.3.1.a-1: AT&T Infrastructure Protection Methods. Agencies benefit from an infrastructure that is protected through a rigorous set of security methods, processes, techniques, and practices that minimize threats.

The services provided to the Agencies are shielded from security threats because AT&T follows best practices and incorporates extensive security methods to protect our network infrastructure. AT&T maintains an ongoing security practice with the U.S. Government and welcomes the opportunity to expand that practice with the Agencies.

1.3.1.b Measures to Protect Against Cyber Attacks

[L.34.1.3.1.b]

(b) Describe the measures to provide protection to the offeror's infrastructure against cyber attacks (e.g., Denial of Service (DoS), Domain Name Server (DNS), and SS7 attacks, Spoofing, routing table corruption).



As a global communications carrier, AT&T has a twofold security environment to manage: (1) its own enterprise computing environment, and (2) the systems and equipment of its global network infrastructure. AT&T develops security innovations and deploys them on its corporate Intranet first. Next, it leverages those innovations and brings them to its various service networks. Finally, it uses them to assist enterprise customers with their own security management challenges.

1.3.1.b.1 Network Management Security Protection Methods

Table 1.3.1.b-1 lists how we protect our network and the services that we offer to Agencies in the categories of enterprise network management, IP network configuration management, and automated network provisioning and configuration tools. Agencies will benefit from the security that AT&T applies to

Stopping cyber attacks in the network will mitigate cyber attacks on Agencies' applications.

its network and services from AT&T's ability to thwart attempted intrusions to the network and AT&T's services. In those cases where

engineering and implementation are required for security services, AT&T deploys protections and disciplines on Agencies' own internal networks.

AT&T SECURITY PROTECTION METHODS – NETWORK MANAGEMENT
Enterprise Network Management

A comprehensive, multipronged program that provides a disciplined, structured management of AT&T's internal computing assets.

<p>ADVISORY MANAGEMENT</p>	Vendor advisories are categorized for subsequent distribution to AT&T administrators, developers, and system owners [REDACTED]
<p>PATCH VERIFICATION</p>	Patches are applied for networked infrastructure [REDACTED]
<p>INFORMATION REPOSITORY</p>	Information about networked devices enhances the ability to identify and remediate those devices that are vulnerable or infected by a worm or virus [REDACTED]
<p>NETWORK ACCESS CONTROLS</p>	This automated process disconnects vulnerable devices and establishes that only registered devices are allowed to connect to the network [REDACTED]



IP Network Configuration Management

PATCH MANAGEMENT

Deployment of software upgrades or patches is performed in a way that minimizes network disruption to customers and maintains network security and reliability.

Automated Network Provisioning and Configuration Tools

██ provides inventory, provisioning, and automated router configuration functionality for all of AT&T's IP network infrastructure and customer interfaces.

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

Enhances security by reducing the need for manual configuration, which helps to eliminate potential security risks introduced by human error.

████████████████████ manages the configuration of the backbone routers. Automating backbone router configuration reduces potential human error and increases the security and stability of network elements.

A system inserted between the actual routers and the technicians interfacing with it that helps protect the security and integrity of the routers. Development of this tool provides another example of *Defense in Depth*.

Other AT&T automated network management tools for security management.

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

████████████████████ is an AT&T-patented flexible and powerful system that assists in managing and maintaining IP router configurations from an analytical and investigative perspective.

████████████████████ helps detect configuration mistakes and assess the current design of the networks of enterprise customers as well as AT&T's.

This AT&T-patented system monitors the integrity of AT&T route advertisements to external non-AT&T Internet networks².

AT&T-developed software analyzes ██████████ for redundant statements and reduces redundancies, optimizing the router's performance.

Table 1.3.1.b-1: Security Protection Methods Related to Network Management. Agencies directly benefit from AT&T's efforts to protect our own infrastructure against cyber attacks.

1.3.1.b.1.1 Enterprise Network Management

For enterprise network management, AT&T's common security platform (CSP) supports the controlling of access to ██████████ applications. Developed to manage this authentication process, CSP is constructed with ██████████
██
██
██
██
for any application that requires internal network access and/or Internet access. This ██████████
██
is used for AT&T's internal web applications. In building this platform, vendor technology was used to produce an efficient, economical service for applications and demonstrated that such technology is scalable and reliable. The CSP achieved 100-percent availability for over one year, while serving about ██████████ ██████████ per month to AT&T associates and customers.

² The December 5, 2000 issue of Network Magazine described PeerMon as a true differentiator of ISPs.

Web applications save significant expense by avoiding the need to deploy hardware infrastructure into an Internet-facing demilitarized zone (DMZ).

1.3.1.b.1.2 IP Network Configuration Management

For IP network configuration management, AT&T requires that all router software upgrades or patches be certified by a rigorous testing process before deployment in our network. Specific to IP and MPLS, AT&T has built an extensive global test laboratory where all network elements, network integration, services integration, operational support system (OSS) support, and managed CPE support testing is performed. [REDACTED]

[REDACTED] The testing process is rigorous and includes tests for functionality and supportability, as well as for security.

[REDACTED] thus enabling the more rapid deployment of patches across over [REDACTED] AT&T routers globally. With the tool, AT&T will respond more quickly to security advisories and keep its network secure.

1.3.1.b.1.3 Automated Network Provisioning and Configuration Tools

AT&T has automated most network provisioning, management, and configuration tasks, so it built a comprehensive platform with these capabilities. [REDACTED] provides inventory, provisioning, and automated router configuration functionality for all of AT&T's IP network infrastructure and customer interfaces. [REDACTED]

[REDACTED] AT&T has developed automated network management tools that aid in security management (**Table 1.3.1.b-1**).

1.3.1.b.2 Incident Detection Security Protection Mechanisms

AT&T has invested significantly in the development of tools and resources to detect attacks emanating from the global Internet. These tools and resources allow AT&T to predict many Internet events before they became full-blown incidents. This capability protects AT&T's infrastructure and the services that will be provided to Agencies.

Automated tools and well-defined processes allow AT&T to quickly detect and defeat cyber attacks.

Table 1.3.1.b-2 summarizes those Internet-specific security infrastructures.

AT&T SECURITY PROTECTION METHODS – INCIDENT DETECTION/RESPONSE
Internet Incident Detection

AT&T has invested significantly in the development of a suite of tools and technologies to predict many Internet events before they became full-blown incidents.

[REDACTED]	Collects all security-related alerts and advisories into one console [REDACTED]. This AT&T-developed alerts console is monitored [REDACTED] and presents three primary types of information [REDACTED].
[REDACTED]	Analyzes network flow records of IP traffic in the form of IP detail records, together with data relating to Internet network topology [REDACTED].
[REDACTED]	Organizes publicly accessible information, [REDACTED]. This enables rapid analysis of security incidents using graphical representations of information.
DENIAL OF SERVICE (DOS) MITIGATION	Detects and mitigates DoS attacks by a variety of methods, including perimeter black holing (a routing protocol, such as BGP, to divert traffic to a bit bucket in which the packets are discarded before reaching their intended victim) and a technique that diverts traffic to a packet-scrubbing facility that manually or automatically mitigates the malicious packets.
DARK SPACE MONITORING	Observation and studies of dark space yield valuable knowledge of methods for potentially detecting malicious traffic patterns in unused or privately routed address space to listen to Internet and network noise.
WIRELESS SECURITY	Active participating in standards bodies, contributing to the development of strong and effective end-to-end wireless security enable enterprises to use wireless technology fully throughout their organizations in a secure manner. [REDACTED] sampling of network flow data contributes to traffic planning analysis as well as DoS detection and analysis.
[REDACTED]	Monitors network links for use in forensics analysis of security events. [REDACTED]
CONTROL PLANE MONITORING	Monitors activity in the network control plane to identify suspicious topology and routing changes that might be caused by compromised routers.

Table 1.3.1.b-2: AT&T Security Protection Methods Related to Incident Detection and Response. *A variety of tools and technology is used to provide reliable and secure services to Agencies.*

An example of the predictive capabilities of these tools is [REDACTED] [REDACTED] an early tracking of the Sasser worm. In contrast to a spike in traffic arrivals at a specific destination protocol port, Internet worm propagation demonstrates a specific pattern in the number of infected hosts over time that will be detected by an appropriate time-based algorithm.

Figure 1.3.1.b-1 depicts [REDACTED] tracking the early phases of the Sasser worm.

Figure 1.3.1.b-1: Early Phases of the Sasser Worm [REDACTED]

1.3.1.b.3 Incident Response and Remediation Security Protection Mechanisms

The best defense against cyber attacks is early identification and a speedy response.

AT&T has developed security-related resources, both to respond to security incidents affecting AT&T as both an enterprise and a service provider. Several organizations within AT&T respond to suspected security incidents and provide remediation. Their specific areas of expertise and responsibility are detailed below.

- [REDACTED]
provides a reliable, trusted, single point-of-contact within the company for security events and emergencies. The [REDACTED] is available on a 24x7 basis. Corporate policy requires that AT&T personnel notify [REDACTED] if a computer, computer system, or network has been compromised, or if a breach of security is suspected. Additionally, [REDACTED] monitor all the intrusion detection activity at [REDACTED].
[REDACTED] These incidents are tracked [REDACTED].
[REDACTED] will confirm the incident and coordinate all investigative and recovery efforts. After it has resolved the incident [REDACTED] conducts a post-mortem to identify any gaps in the process and gain credible data to foster improved decision making (e.g., architectural design, policy, operational procedures, etc.). An incident cannot be closed until the post-mortem has been completed.
- For critical (Severity-1) outages, managers [REDACTED] establish [REDACTED] between the Situation Manager and relevant managers. The purpose of the [REDACTED] is to identify the problem and the AT&T organization leading the recovery, describe the impact on AT&T business units and customers, identify the root cause of the outage, describe the recovery plan, and provide an estimated time to restore (TTR) service.

An example of this type of security incident was the Slammer worm that rolled across the Internet in January 2003. [REDACTED] saw the dramatic increase in traffic across our IP network, and an [REDACTED] was initiated. [REDACTED]

[REDACTED]

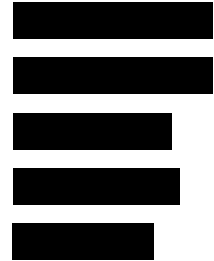
AT&T will be able to detect preliminary attempts, in advance, rather than being caught unaware. **Figure 1.3.1.b-2** shows a [REDACTED]

configuration changes. Security vulnerabilities introduced by human errors are minimized through automated provisioning and configuration tools. Network vulnerabilities, such as peering points, are closely monitored through tools, such as [REDACTED]

If a cyber attack, such as a DoS, breaches the proactive defenses, then AT&T's many incident detection and response systems quickly identify and mitigate the threat. The incident detection systems collect network flow data, firewall logs, alarms, tarpits, honeypots, and other pertinent data from inside and outside the network. All the incident data is aggregated and correlated [REDACTED] [REDACTED] so network operations personnel are able to assess and react to the situation quickly. Configuration and topology databases, [REDACTED] [REDACTED] allow operations personnel to quickly gather the necessary data about the vulnerable network device(s) to mitigate the cyber attack.

Finally, system hardening is among the primary tools used to protect systems against security threats. AT&T's systems hardening includes the removal of all unneeded system tools and processes, so that the systems software has been developed using acceptable security practices; old versions of software and test software test tools are not included in the active service build. In addition, service updates are fully tested for security and deployed only in a hardened configuration that includes automated updates to eliminate security holes due to human error.

1.3.1.b.5 Customer Security Protection Mechanisms



AT&T has moved security intelligence into its IP network on the new AT&T Internet Protect service

Figure 1.3.1.b-3: AT&T Internet Protect 

(**Figure 1.3.1.b-3**). This service provides a network-based solution for intrusion detection systems (IDS), firewalls, and anti-virus and anti-spam systems. This service contrasts to the industry practice of distributing security solutions at the edge of the IP network, which is costly to clients, inefficient, and repetitive across the client base.

AT&T Internet Protect clients receive security alerting and notification service, providing advance warning of potential attacks, including viruses, worms, and DoS attacks.

Agencies are notified by pager and a secure web portal within minutes of this activity, and provided

recommendations for immediate action. AT&T Internet Protect also delivers essential security information, such as top vulnerabilities, recent patch releases, and other need-to-know facts. AT&T has also announced an additional capability as an add-on option to Internet Protect. Distributed denial of service (DDoS) defense alerts Agencies who are the targets of an attack and removes the attacking data

Integrating detection, analysis and notification of cyber events is a powerful security service for Agencies.

streams from their overall traffic. DDoS defense provides that Agencies receive only the traffic that they should receive, helping to protect against the disruption caused by DDoS attacks.

Agencies benefit from the security measures (described above) to provide protection against cyber attacks to AT&T's infrastructure. Those benefits are extended to AT&T's managed security services, which will help guard Agencies' networks against hostile attacks. AT&T's approach to security considers the sum total of protections offered in the separate security services and how those will best be used to provide a greater degree of security protection more cost effectively.

For example, data gathered in the managed firewall service will be used as input for the processing performed in the intrusion detection and prevention service. Similarly, alerts and possible security incidents discovered in the intrusion detection and prevention service will provide timely and meaningful inputs to the incident response service. **Figure 1.3.1.b-4** depicts AT&T's approach to providing Agencies with comprehensive security protections in a cost-effective manner.

Figure 1.3.1.b-4: AT&T's Integrated Managed Security Services. Agencies' networks are protected by AT&T's approach to security using its suite of managed security services.

1.3.1.c Application of Security and Reliability Best Practices [L.34.1.3.1.c]

(c) Describe how the network architecture is consistent with best practices for security and reliability.

AT&T's security expertise exemplifies the due diligence and discipline that a service provider can take to successfully protect its network and computing

infrastructures, as well as those of Agencies.

By following Security Best Practices, AT&T continues to thwart future security attacks.

AT&T uses industry standards and our own best practices when designing methods and

procedures to provide safe, reliable services. AT&T's expertise was demonstrated by its ability to ward off the MS-SQL worm attack, which slowed global Internet traffic to a crawl for millions of users on hundreds of ISP networks in January 2003. AT&T also gave advance warning to its

Internet Protect customers about attempts that became the Sasser worm in May 2004. **Table 1.3.1.c-1** describes AT&T's basic principles for providing safe, reliable services.

AT&T SECURITY BASIC PRINCIPLES	
DEFENSE-IN-DEPTH	One of AT&T's fundamental security design principles provides that many integrated mechanisms with multiple levels of protection against attacks.
PREVENTION	AT&T focuses on preventing network attacks by designing security into every AT&T network and service from the start to enhance the security of its network, systems, and services against all known attacks.
SECURITY MANAGEMENT	AT&T is focused on deploying a variety of methods and systems for dealing with the evolving security environment, including software management and system integrity; configuration management, traffic measurement, and detection; response and mitigation; and post-event analysis and remediation. As part of this effort, AT&T is moving intelligence into the IP network to eliminate the costly inefficiencies of deploying security solutions at the edge of the network.
INNOVATION TRANSFER	AT&T has long had a practice of developing and implementing security innovations on its enterprise network first, and then extending those technologies to its networks and services provided to customers.

Table 1.3.1.c-1: AT&T Security Basic Principles. *These basic principles guide AT&T's efforts to design security in our network and services.*

AT&T follows a well-defined process for designing security into every service or feature, from security architecture to deployment. AT&T also uses the principle of domain separation to protect its internal networks and those of its customers. By hardening its network elements against attack in accordance with vendor, industry, and internal recommendations, more security is achieved. AT&T has developed tools to monitor its network infrastructure for unauthorized changes and attacks caused by worms and viruses.

Table 1.3.1.c-2 summarizes the best practices AT&T uses for designing in security, using prevention by design.

AT&T PROTECTION METHODS – DESIGNING IN SECURITY	
██████████	<ul style="list-style-type: none"> • AT&T Security Policy and Requirements (ASPR) govern security in all AT&T services from operating systems to operations. • AT&T ██████████ ensures security is embedded into every step of service development and network deployment, including architecture, requirements, reviews, testing, monitoring, maintenance, and incident response.
DOMAIN SEPARATION	<ul style="list-style-type: none"> • For AT&T's internal networks and managing customers' networks. Domain separation limits communications between domains as authorized, through designated gateways that will detect suspicious activity and block it. • Allows communications between two domains to occur in a tightly controlled manner, through only a few communication points and under close scrutiny based on type of traffic, source, destination, and volume of traffic. • Points of presence (Central Offices) are built with multiple security zones. • Hosting data center architecture includes several logical zones for security

HARDENING
INFRASTRUCTURE
ELEMENTS

- so that traffic cannot leak between zones.
- All servers are hardened per vendor, industry, and internal recommendations.
- Host-based agents continuously monitor the servers looking for unauthorized changes in software and configurations.
- AT&T deploys measures to protect against DoS attacks at the host and element level, network level, and service (application) level.
- AT&T Internet Protect monitors IP traffic for new attacks, such as those caused by worms and viruses.
- All these systems are monitored [REDACTED]
- Strict boundaries are defined regarding which device will communicate with which device, providing additional control.
- A border element (BE) has been defined within the AT&T services over IP architecture, providing an additional layer of security beyond that inherent within VoIP devices. BE acts as an intermediary between the trusted domain and the untrusted domain.
- Using the BE, AT&T has protected services over its IP call processing and management infrastructure by multiple firewalls that create a DMZ between its BEs and the call control elements (CCEs) within a separate trusted domain.

SEPARATE SERVICES OVER
IP INFRASTRUCTURE

Table 1.3.1.c-2: AT&T Protection Methods. Agencies will benefit from AT&T's prevention by design method from the beginning of the development process to securing its network and services.

1.3.1.d Approach to Incorporating Security Enhancements [L.34.1.3.1.d]

(d) Describe the approach for incorporating into the offeror's network, infrastructure security enhancements that the offeror believes are likely to become commercially available in the timeframe covered by this acquisition. Include a discussion of potential problems and solutions.

Security continues to be critical in this new era to counter the growing threat of attacks from ever-more sophisticated cyber terrorists and criminals. With continued commitment to security discipline, AT&T develops new practices and technologies that enhance security. In addition, many vendors develop new technologies to enhance security, on all possible fronts. These include embedding security into all computing and networking devices, developing smart agents to spot troubles and respond immediately, and building self-healing capabilities into systems and networks. AT&T's approach to future security enhancements is described in **Table 1.3.1.d-1**.

THE NETWORK AS A
SECURITY DEVICE

ANTICIPATED SECURITY ENHANCEMENTS

- Security (i.e., firewall, antivirus, etc.) migrate from edge devices to the network
- Network-based security functional areas are integrated into a single security tool
- Network becomes increasing intelligent in identifying and mitigating security threats
- Network becomes a security device for the Agencies
- Quantity of IP-based services will expand during Networx contract
- Application specific security capabilities will be developed for each new

SECURING SERVICES
OVER IP

SECURING NETWORK STORAGE	service
SECURING MOBILE AND REMOTE USERS	<ul style="list-style-type: none">• Consolidation of user data on network-based storage presents security threat• Intelligent applications and situational aware-sensors must be applied to network storage to protect Agencies• Storage system restoration and backup are mandatory to protect user data• Proliferation of subscriber devices• Authenticate authorize subscribers• Secure transport required because of dependency on network storage
NETWORK-BASE IDENTITY SYSTEMS	<ul style="list-style-type: none">• Identity management systems to verify information exchange• Network-based Identity systems reduce Identity theft risks• Works across multiple subscriber devices (i.e., personal digital assistant [PDA], personal computer [PC], cell phone)• Security needs and privacy concerns must be balanced

Table 1.3.1.d-1: Anticipated Security Enhancements. *To address future security challenges, Agencies increasingly rely on the network to act like a security device. A continued commitment to security discipline allows continued development of new practices and technologies to enhance security.*

1.3.1.d.1 Services over IP security

Over the term of the contract, the Agency can anticipate that AT&T will continue to introduce innovative security technologies into the network. Security innovations underway within AT&T laboratories are focused on shifting security away from the network perimeter to the *cloud*. Through careful deployment of intelligent applications and situational aware sensors, network attacks and malicious code will be detected in the cloud well before the attack or malicious code has an opportunity to hit the network perimeter. Intelligent sensors and applications will provide analysts with near real-time intelligence, which will enable rapid deployment of defensive countermeasure.

For example, the emerging area of VoIP analysts is already predicting an onslaught of spam over IP telephony (SPIT). [REDACTED]

1.3.1.d.2 Storage Area Networks

Storage area network (SAN) is a popular tool offering a growing availability of bandwidth and a growing dependency on the data available on our systems' remote backup services. This is likely to become popular, especially with

distributed mobile workforces. Without proper security measures, these backup facilities can represent a very real threat to the data security of a company. Although the obvious solution might be to prohibit the use of SANs; however, with the increased reliance on mobile devices, it might be essential to back up and restore systems securely and remotely to provide business continuity and protect company assets. Intelligent applications and situational aware-sensors can prevent attacks before it reaches the core assets. At the same time, these tools can allow users to securely restore systems from remote locations.

1.3.1.d.3 Mobile and Remote Users

Looking into the future, the growing availability of high-speed mobile connections allows users to always be in connection with information. Small devices can be effortlessly networked with large data stores back at the home office. With increasing reliance on data stored remotely, the availability and integrity of the data are essential. Depending on the type of data, privacy can be critical as well. Not only must the data store be protected, but also the data in transit must be protected from modification and corruption both to and from the user. AT&T already has advanced DDoS protection systems and is known for its reliable networks. As the network becomes more distributed, self-healing and self-aware networks are critical for providing the availability, integrity, and privacy of data stored in memory enhancement devices.

1.3.1.d.4 Identity Systems

As the network and real world continue to overlap and enhance each other, identity will become a significant issue. Not only will identity be critical for users to access their data remotely, but also interchanges between people or systems will need a reliable form of identity management that, at the same time, does not reveal too much information. What information to exchange in a particular setting will need to be modulated, depending on whom a person

is communicating with – are they a fellow employee, someone on the same project, someone from another company – and what information is accepted will need to be modulated.

Having a reliable identity system can provide the appropriate level of disclosure and prevent potential damage by confining access to information based on identity. Because many end point devices (phone, PDA, etc.) need to provide the users' identity, the common solution is to insert the identity technology into the user device. However, assigning identity components to the end device creates both a security risk and inconvenience for the subscriber. End user devices can be stolen or lost. Subscribers must also have the end device to be identified by the network. For identity systems to operate effectively, they must not rely on the end device to verify the users' identity. The only way to provide a secure adaptable identity system is by moving the intelligence to the network.

AT&T is committed to developing new network-based security services, such as an identity system network. AT&T has developed numerous security innovations and management techniques supporting security and has leveraged these security innovations to create services to support enterprises. AT&T's commitment to security will continue well into the 21st century, as security will become increasingly challenging. Based on these technology trends, AT&T predicts the emergence of a global, virtual society. In this society, mobility will be the norm as businesses and consumers demand a multitude of digital services that can be accessed from anywhere, at anytime, and by anyone (or by anything, e.g., appliances) over IP networks.

1.3.1.e Certification and Accreditation (C&A) Experience [L.34.1.3.1.e]

(e) Describe the offeror's experience in supporting the Government in developing the documentation required in the Certification and Accreditation (C&A) process. (see National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) PUB 800-37 — Guide for the Security Certification and Accreditation of Federal Information Systems).

The goal of the C&A process is to verify that the system to be certified and accredited does have the proper security configurations implemented to support its mission. The certification process provides the person accrediting the system with the documentation to make the accreditation decision. The objective of AT&T's Information Assurance (IA) is to achieve the necessary accreditation by working with the Agency through each step of the certification process. AT&T verifies that all the required security configurations and processes are properly in place and well documented. Our capabilities for achieving that goal are summarized in **Table 1.3.1.e-1**.

EXPERIENCE DEVELOPING DOCUMENTATION FOR CERTIFICATION & ACCREDITATION	
PERSONNEL – CLEARED, TRAINED, AND EXPERIENCED	<ul style="list-style-type: none"> • Secret, Top Secret (TS) and Top Secret/Sensitive Compartmented Information (TS/SCI) Personnel • Skilled Personnel with Certified Training <ul style="list-style-type: none"> • Certified Information System Security Professionals (CISSP) <ul style="list-style-type: none"> • Information Systems Security Engineering Professional (ISSEP) • Information Systems Security Architecture Professional (ISSAP) • Information Systems Security Management Professional (ISSMP) • Certified Information Security Manager (ISM) – IS Audit and Control Association • Global Information Assurance Certification (GIAC) Certified Intrusion Analyst (GCIA) – SANS) • Dedicated Hosting Service (DHS) Level III Certification • Cisco Certified Network Administrators/Professionals (CCNA/CCNP) • Microsoft Certified Systems Engineer (MCSE) • Advanced Degrees – PhD, MSEE, MS
FEDERAL GUIDELINES AND PROCESSES	<ul style="list-style-type: none"> • Performed C&A work from Phase 0 (Questionnaire) to Approval-to-Operate (ATO) • C&A Methodology based on NIST FIPS Publication 800-37 • C&A Methodology Complies with OMB Circular A-130; • Follows DoD Information Technology Security Certification and Accreditation Process (DITSCAP) for DoD Agencies. • Follows Intelligence Community C&A processes (National Information Technology Security Certification and Accreditation Process [NISTCAP]; National Information Security Certification and Accreditation Process [NISCAP]; National Information Assurance Certification and Accreditation Process [NIACAP]; Northern Regional Operations Center [NROC])
COMPREHENSIVE C&A DOCUMENTATION AND TOOLS	<ul style="list-style-type: none"> • Provide Comprehensive Documentation Set – Security Questionnaire, Security System Plan Security Traceability Matrix, Security Test & Evaluation; Risk Assessment; Configuration Management, Security Features Users Guide, etc.

- C&A Tools – Information System Analysis and Requirements (ISAR) tool
 - Facilitates Information Domain Development and Security Requirement Traceability Matrix
 - Documents and Produces Node Topology and Data Flows
 - Produces the Security System Plan, Requirements Matrix and Common Criteria Equivalent Requirements
 - Follows DITSCAP, NISCAP and NIACAP, and Director of Central Intelligence Directive (DCID) 6/3 Guidelines

C&A EXPERIENCE C&A customer base includes, but is not limited to, [REDACTED]

Table 1.3.1.e-1: AT&T Certification & Accreditation Experience. *The development of documentation required in the C&A process calls for strict adherence to Federal guidelines. Agencies are supported by the extensive C&A experience that the AT&T Team of skilled personnel offers.*

1.3.1.e.1 AT&T Information Assurance (IA) Team

AT&T's Information Assurance (IA) Team is composed of experts with advanced technical degrees (BS, MS, MSEE, PhD, etc.); who have certifications (Certified Information Systems Security Professional [CISSP], Cisco Certified Network Administrator [CCNA], Microsoft Certified Systems Engineer [MCSE], and Project Management Professionals [PMP] certifications, etc.); and who hold the appropriate security clearances (Secret, Top Secret, or TS/SCI).

The IA security team members also have extensive and diverse backgrounds in systems administration, network administration, network engineering, security engineering, architecture design, and protocol and traffic analysis. Their understanding of networks and how systems communicate allows them to leverage analytical information to conduct security analyses and develop proper processes/procedures to meet specific customer needs.

1.3.1.e.2 C&A Guidelines

AT&T's security certification embraces the NIST FIPS Publication 800-37 (*Guidelines for Security Certification and Accreditation of IT Systems*) methodology, as required by Office of Management and Budget (OMB) Circular A-130, Appendix III. Depending on the Agency's requirement, the C&A process, followed by the AT&T IA Team, might be one of the following: DITSCAP, NISCAP, NIACAP, or NROC. The IA Team's experience with and

knowledge of the C&A guidelines allow them to perform the required tasks and assemble the appropriate documentation to assist an Agency with achieving authority to operate (ATO) status.

1.3.1.e.3 C&A Documents and Tools

Agencies will obtain the documentation necessary to complete C&A within the Federal Information Security Management Act (FISMA) of 2002 mandated, three-year cycle of C&A activities, including evidence of security compliance and C&A documentation, as defined within the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 guidance. The AT&T IA Team has extensive experience in assembling all required documentation to support a full C&A effort (**Table 1.3.1.e-2**).

PHASE 0 QUESTIONNAIRE	Phase 1 Checklist	Capability Maturity Model (CMM) System Security Policy
SYSTEM SECURITY CONCEPT OF OPERATION (CONOP)	System Security Plan (SSP)	Security Requirements Traceability Matrix (SRTM)
SECURITY TRAINING AWARENESS PLAN	Trusted Facility Manual (TFM)	Security Features Users Guide (SFUG)
CONFIGURATION MANAGEMENT (CM) POLICIES AND PROCEDURES	Configuration Management (CM) Plan	Incident Reporting Plan and Procedures
INCIDENT RESPONSE PROCEDURES	Backup and Restoration Plan (BU&R)	Continuity of Operations/ Disaster Recovery
INTERCONNECTION SECURITY AGREEMENT (ISA)	Security Test Plan and Procedures	Risk Assessment (RA)

Table 1.3.1.e-2: AT&T C&A Documentation Preparation. Agencies can rely on the AT&T Team to prepare and assemble the documentation required in a full C&A effort.

To facilitate the complicated C&A documentation preparation process, AT&T developed [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Figure

1.3.1.e-1 [REDACTED]

1.3.1.e.4 C&A Experience

AT&T IA Team has performed C&A activities from the beginning of the C&A Phase 0 Questionnaire through achieving full ATO. Agencies benefit from our C&A experience that includes architecture

Figure 1.3.1.e-1: [REDACTED] Security Engineering Tool. [REDACTED]

design through development, implementation of systems at various levels, identifying the security requirements, auditing, and other C&A required services.

Beyond assembling the C&A documentation, the IA Team has provided assistance with security architecture, security policy, security planning/requirements definition, prototyping and testing, product selection, deployment and ongoing support, and organizational structure analysis and recommendations. Additionally, AT&T's IA Team has well-established experience in performing DCID 6/3 C&A work to certify systems and architectures, such as PL2 and PL3. Understanding the requirement is critical to developing a system that is secure, compliant with DCID 6/3, and matches the Agency-specific mission(s). If necessary, the AT&T IA Team will conduct the comparisons between the DCID 6/3 requirements and DITSCAP/NIACAP



security requirements. The C&A past experience includes serving the following clients:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]