1.6.6 Incident Response Service (INRS) [C.2.10.5]

The Incident Response Service (INRS) will provide highly effective detection, protection, and mitigation capabilities to safeguard Agency critical infrastructure elements and assets in the face of cyber attacks and cyber security threats. Agencies will receive state-of-the-art systems and tools developed by AT&T Labs and tried and tested through the global AT&T network. Agencies will also receive dedicated support from leading industry security professionals working from state-of-the-art network monitoring and security response facilities.

1.6.6.1 Technical Approach to Security Services Delivery [L.34.1.6.1]

"For implementing extremely flexible management offerings, being the first to bring application security services to the market, and offering the widest array of services in the industry, AT&T [Managed Security Services], is awarded the Customer Solutions Excellence Award."

--Frost & Sullivan July 2003.

1.6.6.1.a Approach to Service Delivery [L.34.1.6.1.a]

(a) Analyze the service requirements specified in this solicitation and describe the approaches to service delivery for each service. [L.34.1.6.1.a]

Agencies use INRS to protect IT and networking resources from cyber attacks and crimes. Agencies require compliant INRS solutions with:

- INRS as an integrated component of an overall sophisticated security framework
- A service that is both proactive and reactive
- Considerable vendor assistance and support during the entire INRS lifecycle:
  - Planning and assessment prior to an attack or actionable threat
  - Thwarting, protecting, and restoration during the attack or actionable threat

- Forensics and lessons learned post attack or actionable threat

AT&T is uniquely positioned to offer Agencies INRS that meets these three broad requirements and more importantly, help Agencies use INRS to raise the overall understanding and impact of security upon the Agency's mission and business mandates. In a similar fashion, AT&T has used it to become the leader and a vocal proponent of security and its importance within the government and business enterprise[1].

AT&T presented Customers Solutions Excellence Award for Managed Security Services- for the second consecutive year. AT&T "reigns as the single most prolific MSSP in the market."

--Frost & Sullivan
October 2004

Agencies receive a robust INRS offering through the following attributes, which in combination have allowed AT&T to deliver advanced and comprehensive security solutions to secure both the internal global AT&T network as well as many large government and enterprise networks:

- The sheer scale of the AT&T global IP network and its extensive peering. This "live test bed" provides AT&T security organizations with first visibility into the happenings of the public Internet
- The AT&T Global Network Operations Center (GNOC) that aggregates all AT&T network management and operations centers and that has complete overall visibility into all AT&T networks
- The depth and breadth of expertise available at the AT&T Labs organization, with its more than [redacted] responsible for designing, deploying, and integrating a number of highly advanced security tools and systems [redacted]

[1] *Dr. Ed Amoroso, AT&T's noted Chief Security Officer, is regarded within the industry as one of the visionaries and proponents of "network integrated security" a concept that has allowed AT&T to become one of the most secure network providers in the industry.*

- The AT&T [redacted] which plays a vital role in helping AT&T remain vigilant and adapted to the ever-changing security landscape
- A spectrum of intelligent, scalable, and tried-and-tested systems that collect, process, and analyze very large amounts of data traffic in real-time and present data, information, and knowledge to AT&T security organizations and Agencies

In addition to these broad INRS enablers, Agencies receive compliant and a leading INRS through the following specific service elements:

- The [redacted]
- The Internet Protect portal
- The distributed denial of service (DDOS) defense service
- The Incident Response Team (IRT)
- Professional security services

Figure 1.6.6.1-1 depicts the above components within INRS.

Agencies receive a comprehensive INRS service that is inclusive of a number of critical elements that in conjunction help Agencies protect critical IT and networking resources. AT&T's approach (**Table 1.6.6.1-1**) to service delivery of INRS is based upon the broad factors mentioned above and reflects our experience providing large-scale, secure enterprise networking solutions to large government entities and enterprises.

Figure 1.6.6.1-1: INRS Service Components:. *The Agency will meet its need through INRS for a service that responds to potential malicious attacks and service disruptions.*

SERVICE DELIVERY APPROACH	TECHNICAL DESCRIPTION
Compliance with leading government and commercial standards	• E-Government Act of 2002, Title III—Federal Information Security Management Act (FISMA) • Internet Engineering Task Force (IETF) RFC 2350—Expectations for Computer Security Incident Response • National Institute of Standards and Technology (NIST) Standards • United States Computer Emergency Response Team/Coordination Center (US-CERT/CC) reporting requirements • Sarbanes-Oxley requirements • World Wide Web Consortium (W3C) standards and guidelines • Forum of International Response and Security Teams (FIRST)
Proactive service	INRS includes key proactive activities: strategic planning, policy and procedure, vulnerability assessment, preventive analysis, and recommendations, and training
Advanced information processing systems	• Systems spanning all elements of a comprehensive SIM: situational awareness, actionable alerts, case management, advisories, metrics, daily management, and cyber intelligence flash reports. • Systems incorporate Decision Support System (DSS) and Correlation Engine (CE) that intelligently process very large amounts of data from servers, firewalls, networking devices, agents, databases, and data aggregators. DSS and CE reduce a large number of security events to a significantly smaller number of “actionable” items while minimizing false positives • Designed to support long interval data mining and event correlation through AT&T Labs developed database systems

SERVICE DELIVERY APPROACH	TECHNICAL DESCRIPTION
Network integrated security and defense in depth	• Unique AT&T approach that builds upon the vast amounts of data traveling through one of the largest Internet networks, extensive peering, thousands of service nodes, and tens of thousands of managed devices • The "network" is an integral component of sound security. • Allowed AT&T to detect and neutralize large scale mission and business impacting threats
Organization and personnel expertise	Most important asset in helping Agencies protect key infrastructure elements and includes personnel and expertise from: AT&T Labs, the AT&T Security Center of Excellence (SCOE), INRS team, GNOC, AT&T Professional Services, and AT&T Government Solutions

Table 1.6.6.1-1: INRS Capabilities. *INRS provides proactive capabilities, reactive capabilities, and premium security consulting services to alert Agencies to possible attacks on their network before they affect service availability.*

AT&T's INRS service is designed and deployed with the goal of providing high-quality, secure, and technologically superior solutions on a global basis. This approach has allowed AT&T to become the industry leader in providing secure enterprise networking solutions.

1.6.6.1.b Benefits to Technical Approach [L.34.1.6.1.b]

(b) Describe the expected benefits of the offeror's technical approach, to include how the services offered will facilitate Federal Enterprise Architecture objectives (see http://www.whitehouse.gov/omb/egov/a-1-fea.html). [L.34.1.6.1.b]

AT&T's Networx services, in general, and INRS services, in particular, support the Government's vision of transformation through the use of the Federal Enterprise Architecture (FEA) to use technologies to contribute to mission performance. **Table 1.6.6.1-2** describes each service-delivery approach element in relation to FEA and summarizes its contribution and/or provides an example of how it facilitates FEA implementation. AT&T is aligning its product and service components to be easily integrated, commonly manageable, and usable. This applies across Government functions, horizontally and vertically, as well as between levels of government.

SERVICE DELIVERY APPROACH/ FEATURE	BENEFITS	FEA FACILITATION
Compliance with leading government and commercial standards	INRS consistently conforms with the established best government and commercial practices	Facilitates communication and collaboration between Agencies and minimizes information barriers
Proactive service	Allows Agencies to become better prepared for attacks and minimize damage to Agency resources during and after attacks	Allows Agencies to minimize costs associated with responding to network wide threats and damage

SERVICE DELIVERY APPROACH/ FEATURE	BENEFITS	FEA FACILITATION
Advanced information processing systems	Allows AT&T and Agencies to gather crucial knowledge and intelligence at a very early stage to thwart and minimize damage	Allows Agencies to better plan and align large scale IT and networking resources to mission and business objectives
Network integrated security and defense in depth	Agencies benefits by adding a highly functional and economical security layer to existing network protection mechanisms	Allows for adoption of remote access and telework solutions that allow Agencies to better respond during times of crises
Organization and personnel expertise	Allows Agencies to keep up to date with the dynamic network security market and free up internal resources and training of network security specialists.	Allows Agencies to minimize waste and duplication and better emphasis on Agency core mission and business requirements

Table 1.6.6.1-2: INRS Component Benefits. *The INRS benefits will support the Networx program goals to provide security from cyber attacks and provide a cost-effective solution to the Agency's incident response needs.*

AT&T's has developed net-centric technologies that support solutions based on service-oriented architecture (SOA) that uses standardized, web-adapted components. Our approach provides that:

- Technical Reference Model capabilities are fully met and linked to the Service Component Reference Model (SRM) and Data Reference Model (DRM).
- These links are structured to support Business Reference Model (BRM) functions and link Performance Reference Model (PRM) line-of-sight link to mission performance and ultimate accomplishment.
- AT&T operates as an innovative partner through Networx to help achieve the vision of the FEA to enhance Agency mission performance.

1.6.6.1.c Major Issue to Service Delivery [L.34.1.6.1.c]

(c) Describe the problems that could be encountered in meeting individual service requirements, and propose solutions to any foreseen problems. [L.34.1.6.1.c]

In transitioning into any new service delivery model, whether it be task-based or fully outsourced, unforeseen issues can always arise. Therefore, it is important that GSA select a service provider that brings the depth and background to minimize an Agency's risk during transition. Our experience has enabled us to develop proven methods, processes, and procedures applicable to the simplest to the most complex projects.

Table 1.6.6.1-3 lists the top four service delivery risks and our mitigation strategy. As with all large, incident response projects, we enter each of these risks and others (after identification and characterization) into our risk-tracking database, and immediately take steps to mitigate them before they become an issue. Because risk management is more effective when all stakeholders are active in the process, AT&T engages the GSA, the client Agency, and other Government solution partners for success with risk mitigation activities.

RISK	DESCRIPTION	RISK MITIGATION
External security threats	Security threats in the form of worms, viruses and other threats that emanate from the Internet may cause severe damage to Agency critical resources.	AT&T Implements "network integrated security": • Collect, process, and analyze vast amounts of public IP packets • Take action when necessary • Share knowledge and intelligence with Agencies
Internal security threats	Security threats emanating from within the Agency	INRS supports both external threats as well as threats emanating from internal sources
Untimely response times	Timely response to attacks and threats minimizing damage and compromise of Agency resources	INRS compliant with required response times
Business disruption	Business disruption associated with outsourcing key IT and networking functions to a managed services provider.	• Develop engineering design in conjunction with the Agency that considers equipment replacement, concurrent operations, and break-in period • Lab-test all service delivery processes and procedures • Plan for possible contingencies • Possess detailed fallback procedures • Conduct delivery activities during non-business hours, as directed by Agency site POC.

Table 1.6.6.1-3: Risk Mitigation to Service Delivery. *INRS will provide timely service, allowing the Agency to concentrate on core business issues.*

AT&T has taken steps to identify risk and provide risk mitigation associated with delivering INRS. AT&T is committed to service excellence and will work with the Agency to identify and resolve potential problems that might occur during service delivery.

1.6.6.2 Satisfaction of Security Services Performance Requirements [L.34.1.6.2]

1.6.6.2.a Service Quality and Performance [L.34.1.6.2.a]

(a) Describe the quality of the services with respect to the performance metrics specified in Section C.2 Technical Requirements for each service. [L.34.1.6.2.a]

Government Agencies will access the highest quality INRS. AT&T will [redacted] of key performance indicators (KPIs) for INRS for routine and critical users as presented in the RFP and in **Table 1.6.6.2-1**.

KPI	SERVICE LEVEL	PERFORMANCE STANDARD (LEVEL/THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
On-Site Incident Response	Routine	Within 36 hours of the notification for a Low category incident Within 24 hours of the notification for a High category incident	[redacted]
Telephone Incident Response	Routine	Within 1 hour of the notification for a Low category incident Within 15 minutes of the notification for a High category incident	[redacted]

Table 1.6.6.2-1: Performance Metrics for INRS. *INRS will respond to repel malicious incidents and avoid service disruptions.*

AT&T's confidence in the ability to deliver these performance results is supported by AT&T's performance metrics in supporting, securing, and protecting its large internal global network and those of its government and enterprise customers backed by stringent service credits.

1.6.6.2.b Approach to Monitoring and Measuring Performance [L.34.1.6.2.b]

(b) Describe the approach for monitoring and measuring the Key Performance Indicators (KPIs) and Acceptable Quality Levels (AQLs) that will ensure the services delivered are meeting the performance requirements. [L.34.1.6.2.b]

Of equal importance to identifying the KPIs for a service is the method by which the KPIs are captured, measured, and monitored. AT&T monitors the KPIs within our [redacted] (SOC) using our automated [redacted] maintaining them within the guidelines of the AQLs. **Table 1.6.6.2-2** provides a description of the approach to monitoring and measuring of the KPIs, as listed by the Government.

KPI	APPROACH TO MONITORING & MEASURING
On-site incident response	Response measurements are made through the AT&T One Ticketing System (AOTS): • Both reactive and proactive tickets logged.

KPI	APPROACH TO MONITORING & MEASURING
Telephone incident response	• Time elapsed between when a particular ticket was opened (manually via an operator or automatically via one the AT&T automation tools) and closed is used to compute time to restore parameters. • E-bonding capabilities with other ticketing systems (agency or vendor or other provider ticketing systems) • Fault automation (the AT&T ticketing system after performing initial diagnostics automatically, will relay the ticket to the local access provider for speedy fault correction and closure minimizing agency down times) • True integration with other AT&T systems such as those used for KPI verification and executive dashboards.

Table 1.6.6.2-2: AT&T T Monitoring and Measuring Approach. *A one-ticket system maintains availability and time to restore KPIs.*

The first time the service is provided through the Networx contract, the performance must be verified. The KPIs will be monitored to certify that the service performance complies with the AQL. To simplify the verification process, AT&T has automated the process. The common testing platform provides an integrated system to perform service verification testing and present the results either on the AT&T [redacted] web portal or by written report. The service verification process is presented in greater detail in Section 1.3.2.d, Approach to Perform Service Delivery Verification.

1.6.6.2.c Approach to Perform Service Delivery Verification [L.34.1.6.2.c]

(c) Describe the offeror's approach to perform verification of individual services delivered under the contract, in particular the testing procedures to verify acceptable performance and Key Performance Indicator (KPI)/Acceptable Quality Level (AQL) compliance. [L.34.1.6.2.c]

AT&T will conduct [redacted] reviews with the Agency to discuss AT&T's performance, including adherence to contracted performance guarantees. **Table 1.6.6.2-3** describes verification and testing procedures for the KPIs, as listed by the Government. The first time the service is provided through the Networx contract, the service performance must be verified; KPIs will be monitored to certify that the service performance complies with the AQL.

Gartner

Gartner Rates AT&T Highest in 'Ability to Execute' as a Managed Security Service Provider, February, 2003

--as per Gartner's North American MSSP (Managed Security Service Provider)

KPI	VERIFICATION APPROACH	VERIFICATION/TESTING PROCEDURES
On-site incident response	[redacted]	[redacted]
Telephone incident response	[redacted]	[redacted]

Table 1.6.6.2-3: Verification of Acceptable Performance for INRS. *INRS consistently operates above the AQL thresholds and corrective measures are taken expeditiously in the event that these thresholds are missed.*

Through a comprehensive verification process, Agencies and the GSA will receive concrete data that demonstrates the readiness of INRS. AT&T follows detailed procedures to verify INRS, by comparing the KPI data against the stated AQLs, as described in the Verification Test Plan.

1.6.6.2.d Performance Level Improvements [L.34.1.6.2.d]

(d) If the offeror proposes to exceed the Acceptable Quality Levels (AQLs) in the Key Performance Indicators (KPIs) required by the RFP, describe the performance improvements. [L.34.1.6.2.d]

Achieving the Acceptable Quality Levels defined by the Government for the KPIs will result superior INRS performance. AT&T does not propose to exceed the required Acceptable Quality Levels at this time but is open to negotiate AQL values with Agencies on a task-order basis.

1.6.6.2.e Approach and Benefits for Additional Performance Metrics [L.34.1.6.2.e]

(e) Describe the benefits of, and measurement approach for any additional performance metrics proposed. [L.34.1.6.2.e]

The KPIs defined by the Government for the INRS will provide a comprehensive assessment for service verification and service performance monitoring. However, we understand the importance of Agencies needing more comprehensive KPIs and on a task order basis, AT&T analyzes the Agencies' enterprise architecture business objectives and develops more comprehensive KPIs and AQLs.

1.6.6.3 Satisfaction of Security Services Specifications [L.34.1.6.3]

1.6.6.3.a Service Requirements Description [L.34.1.6.3.a]

(a) Provide a technical description of how the service requirements (e.g., capabilities, features, interfaces) are satisfied. [L.34.1.6.3.a]

INRS will be provided to Agencies through a combination of the following INRS service elements:

- The [redacted] system
- The Internet Protect portal
- The Distributed Denial of Service (DDOS) defense service
- The Incident Response Team (IRT)
- Professional security services

The sections below provide a brief description of each of these INRS components.

1.6.6.3.a.1 [redacted]

[redacted] is a fully integrated platform that [redacted] It provides Agencies [redacted] that includes [redacted]

The [redacted] architecture utilizes information from [redacted] It incorporates a [redacted] that allows for [redacted] The architecture is [redacted] and [redacted] and can [redacted] **Figure 1.6.6.3-1** displays the architectural components of [redacted].

Figure 1.6.6.3-1: [redacted] Components. *INRS uses the Aurora system to help protect the Agency against [redacted]*

[redacted] provides a web-based portal interface that unifies the critical network security activities. **Figure 1.6.6.3-2** depicts the top level view of the web portal. The web interface is used to manage the complete lifecycle of security events. For example, the portal provides analysts with actionable alerts that have been collected, stored, and mined from volumes of security information produced by numerous devices. Analysts may drill down to examine the underlying data that comprises any alert. Alerts are correlated to standard operating procedures (SOPs), customized to the Agency's environment, as well as to security advisories gleaned from numerous vendor websites. Alerts are then tracked within [redacted] by an integrated case management tool.

Figure 1.6.6.3-2: [redacted] **Interface.** [redacted] *provides a web interface allowing Agency end users efficient access to security threats and issues.*

In addition to a SIM component, the [redacted] system also incorporates a [redacted] platform that generates alerts based on an analysis of [redacted] derived from traffic traversing [redacted] provides indicators of scans, worm propagation, and DDoS activity as well as volumetric anomalies and network policy violations. As an example of the early warning capabilities provided through [redacted], **Figure 1.6.6.3-3** depicts how the Sasser worm was identified more than two weeks prior to it causing extensive damage to infected systems. AT&T and its customers were able to circumvent such damage due to the powerful inherent capabilities of the [redacted] system.

Figure 1.6.6.3-3: [redacted] Early Detection Capabilities. *The Sasser worm was detected well prior to its causing extensive systems damage.*

With regard to government-defined security policies, the [redacted] product incorporated within [redacted] has already received Common Criteria certification from both NIAP (National Information Assurance Partnership), and CSE (Communications Security Establishment). AT&T is also currently working to certify the remainder of the [redacted] platform components to [redacted] standards.

1.6.6.3.a.2 Internet Protect

World Communication Awards: 'Best Technology Foresight' for AT&T Internet Protect.
--October 2004

Internet Protect is a secure portal that notifies Agencies of Internet-based threats and recommends immediate mitigation actions. It is considered an early warning system that drives its output from intensive data processing of Internet data packets that traverse [redacted] It allows the Agency to be proactive vs. reactive to protect against identified malicious intruders and unauthorized activities. The Internet Protect portal also contains essential security information such as top vulnerabilities, recent patch

releases and other security “need-to-know” facts from a variety of sources. **Figure 1.6.6.3-4** shows a sample Internet Protect screen shot.

Figure 1.6.6.3-4: Internet Protect. *The Agency will be moving to a proactive vs. reactive posture with the Internet Protect DDoS security component of INRS by protecting its network against identified malicious intruders and unauthorized activities. This affords invaluable time to act, typically before any damage is done.*

1.6.6.3.a.3 DDoS Defense Service

AT&T DDoS defense service identifies and mitigates DoS attacks that are directed at Agency IP infrastructure elements. Functions and characteristics include:

- Detects the presence of a DDoS attack and identifies and blocks identified malicious packets in real time without affecting the flow of legitimate Agency traffic.

*"AT&T's DDoS Defense Option for **AT&T Internet Protect further differentiates AT&T's offering** from others in the market, bringing a proactive element to the blend and real time results which competitors will have to take action on to counter, lest they lose business to AT&T."*

--Current Analysis
June, 2004.

- Provides a detailed traffic analysis view and actionable security intelligence specific to the agency VPN. It requires no changes to the Agency network to implement, and will automatically alert detected anomalies. DDOS defense configurations will be applied in accordance with Agency requirements established at the strategic planning period and will be applied within minutes of a potential attack.
- Offered in two configurations. The shared configuration consists of a hardware environment of network detector devices and a farm of network mitigation devices shared among multiple customers. In the dedicated configuration, the network mitigation devices are dedicated to each Agency.
- Compares Agency traffic flows to learned profiles of normal traffic patterns, behavior, and protocol compliance. Traffic delivered to the Agency from the AT&T IP backbone is subjected to a rigorous multi-verification process to remove malicious packets and allow legitimate traffic to pass unimpeded.

Comparing traffic flows to learned profiles of normal traffic patterns, behavior, and protocol compliance, AT&T will quickly and accurately identify and mitigate a broad range of known as well as previously unobserved security attacks, and immediately mitigate a broad range of DDoS threats. When an attack is detected, suspicious traffic is immediately diverted and blocked without disrupting legitimate Agency transactions. AT&T will reroute Agency traffic to the network scrubbing facility within the AT&T network. Traffic will be scrubbed, dropping the DDoS attack traffic, and valid traffic passed to Agency networks. **Figure 1.6.6.3-5** displays the scrubbing process flow.

Figure 1.6.6.3-5: INRS Malicious [redacted] *INRS will filter and block malicious traffic to protect the Agency's network against* [redacted] *attacks.*

AT&T will continue to monitor the scrubbed traffic for DDoS attacks. When AT&T determines that the attack has subsided, AT&T will restore the normal traffic routing and notify the Agency of this change.

1.6.6.3.a.4 Incident Response Team (IRT)

The Incident Response Team (IRT) provides 24x7 response to security threats affecting Agency security resources (**Figure 1.6.6.3-6**). IRT will operate in accordance with the Agency strategy plan and customized response policies and procedures. The team works proactively monitoring anomalies and will notify the Agency of events that may be potential incidents and advise on required actions. The team also provides post-attack investigative and forensics services that assist Agencies in identifying and apprehending offenders.

The team monitors systems for early warnings and reviews security alert information submitted by vendors such as security patches. The team will also

investigate Agency-identified concerns associated with Agency infrastructure, traffic anomalies, and other concerns.

Figure 1.6.6.3-6: [redacted] Operations Center. *Constant monitoring is used to meet the Agency's incident response needs of quick identification and response.*

IRT team members work closely with Agency personnel to set and define measurement parameters such as establishing automated thresholds which trigger automated preventative changes on system components. IRT is an integral component to the overall AT&T INRS defense-in-depth security approach.

1.6.6.3.a.5 AT&T Professional Services

AT&T Professional Services is a talent-rich professional services organization. The organization expertise spans the areas of IT, networking, infrastructure security, COOP/DR, transition planning, technology refresh, as well as other directly and indirectly related disciplines. AT&T Professional Services will assist Agencies in planning and assessment of Agency IT and networking infrastructure security elements. Activities currently supported include training, on-site support, ethical hack, security policy services, and firewall services. Customized services will also be developed based upon each Agency's unique security needs.

1.6.6.3.b Attributes and Values of Service Enhancements [L.34.1.6.3.b]

(b) If the offeror proposes to exceed the specified service requirements (e.g., capabilities, features, interfaces), describe the attributes and value of the proposed service enhancements. [L.34.1.6.3.b]

The built-in security capabilities of Internet Protect and [redacted] extend the basic requirements of INRS. [redacted]

1.6.6.3.c Service Delivery Network Modifications [L.34.1.6.3.c]

(c) Describe any modifications to the network required for delivery of the services. Assess the risk implications of these modifications. [L.34.1.6.3.c]

Agencies receive a low-risk solution by being able to use AT&T's INRS on Day One of the contract because there are no modifications required to the AT&T network or systems to provide INRS services to the Government.

1.6.6.3.d Security Services Experience [L.34.1.6.3.d]

(d) Describe the offeror's experience with delivering the mandatory Security Services described in Section C.2 Technical Requirements. [L.34.1.6.3.d]

> *AT&T received the "2005 Best-in-Class NSP (Network Service Provider) Managed Security Services award."*
>
> --April 2005

AT&T has a long history of providing security solutions that meet the needs of Government organizations – from our lead role in the 1960s Telecom Security program, to our lead role in the 1980s SDI initiative, to our Top Gun program in 2002 (**Table 1.6.6.3-1**). While we cannot name many of our Government customers, some of the nation's most respected enterprises and industry leaders trust AT&T to secure their networks. Our satisfied customer base includes many of the nation's leading Defense and civilian Agencies, as well as large multinational companies like MasterCard and Bank One.

AT&T Need	Solution	Create Value
[redacted]	[redacted]	[redacted]

Table 1.6.6.3-1 Service Experience. *AT&T has an extensive history in providing incident response services to protect our own vast global infrastructure.*

AT&T is actively involved in a wide range of security initiatives from the CEO level. We provide direct support to [redacted] as well as to the many forums, councils, associations, and committees that various AT&T executives, scientists, and professionals serve on. Our security professionals work with a wide variety of government and civilian forums to address some of the United States' most pressing security concerns. AT&T is also involved in supporting various other security related initiatives, including those below, demonstrating our commitment to security at all levels and from all aspects:

- National Security Telecommunications Advisory Committee (NSTAC)
- National Reliability and Interoperability Council (NRIC)
- National Strategy for Cyberspace Security
- National Cyber Security Alliance
- Network Security Information Exchange (NSIE)
- Forum of Incident Response and Security Team (FIRST)

Our active participation in these initiatives enables us to share forthcoming knowledge with our clients, thus better preparing them to comply with new Federal regulations and guidelines. We will share our insights on what is being done in the Federal government arena with our clients so that they can allocate funds for maximum value and benefit.

AT&T offers a "robust set of solutions that is complemented by a strong national brand and resources focused on managed services"… Robust security services including AT&T Internet Protect, a solid managed security solution that supports multiple sensors (e.g., Enterasys, ISS, Cisco, etc.) for clients" and a broad range of other capabilities.

--Current Analysis
December 2004.

For many years, AT&T has led the industry in designing, developing, and deploying security solutions. Our industry leadership spans the spectrum of activities: authoring authoritative books on security topic; the extensive involvement of AT&T representatives in forums, working groups, and associations involved in various security initiatives, such as leading the Internet Engineering Task Force's Security efforts (IETF), and the intense dedication of AT&T's security consultants and operational support personnel in providing security solutions for our government and commercial customers.

1.6.6.4 Stipulated Deviations

AT&T takes neither deviation nor exception to the stipulated requirements.