1.6.3 Intrusion Detection and Prevention Service (IDPS) [C.2.10.2]

Intrusion detection and prevention service (IDPS) uses market-leading security products, combined with advanced analysis performed by AT&T's Managed Security Services expert analyst team, to handle Agency premise-based security monitoring, detection, and prevention. Agencies get unsurpassed value with a fully managed IDPS, which adds another security layer of protection that will be provisioned as a custom service tailored to specific Agency needs.

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

1.6.3.1.a Approach to Service Delivery

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

2004 FROST & SULLIVAN Customer Solutions Excellence Award

"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],"

AT&T was presented the Customer Solutions Excellence Award for Managed Security Services for the second consecutive year, and is awarded the Customer Solutions Excellence Award."

--Frost & Sullivan
July 2003.

Agencies will receive a fully managed, premises and network based, IP network attack recognition and response solution for network security. Intrusion Detection Protection Service (IDPS) provides the same type of protection for networks as a security camera does for physical property. Intrusion detection sensing components are placed at various points at the perimeter and within a customer's network and act as "security cameras" for customer network traffic. The sensing components monitor data packet header and payload information to detect possible malicious activity and respond swiftly with actions based on the customer's pre-defined security posture. **Figure 1.6.3.1-1** illustrates how our IDS is delivered and supported.

Figure 1.6.3.1-1. AT&T Managed Intrusion Detection Service Security Solution. *The Agencies can protect valued resources with IDPS, which is a fully managed, comprehensive, IP network attack- recognition, and response solution for network security.*

Agencies may choose between two IDPS levels. IDPS-Level 2 is a network sensor-centric service based on [redacted] intrusion detection system (IDS) – a managed solution that provides standard analysis and reporting with automated notification and shunning capabilities. For Level 2, Agencies receive a premises-based hardware and software solution that is managed and maintained through the [redacted] Hardware and software maintenance and upgrades are performed routinely or as needed. During the design and engineering stage of service delivery Agencies will have direct input on how the security posture is implemented for each installation.

IDPS-L3 is a network based and sensor-centric service based on [redacted] IDS. A network based IDPS offers security protection before network traffic is forwarded to Agency locations. This layer of security provides another layer of defense and depth protection to Agencies. This service provides advanced analysis and notification with standard reporting. The Agency benefits from a high-quality service that detects and prevents attacks before they enter the Agency's network. IDPS-L3 supports internal network implementation points throughout Agency's entire computing environment including:

Local area networks (LANs)

- Regional peering points
- Partner/customer peering points
- Demilitarization and service zones
- Remote access termination points
- Partner/Agency peering points
- Management, security, and backup networks.

It also supports the traditional perimeter protection implementation points, including inside Agency perimeter firewalls and outside Agency perimeter firewalls. This service is offered as a fully managed service that is managed, upgraded, and maintained through the [redacted]

Table 1.6.3.1-1 highlights our approach to service delivery for both level 2 and 3 IDPS.

SERVICE DELIVERY APPROACH	TECHNICAL DESCRIPTION
Support for standards	Support the following standards as applicable: • E-Government Act of 2002, Title III (Federal Information Security Management Act (FISMA)) • National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) PUB 140 - 2 — Security Requirements for Cryptographic Modules • NIST FIPS PUB 199 — Standards for Security Categorization of Federal Information and Information Systems • NIST Special Publication (SP) 800-31 — Intrusion Detection Systems (IDS) • United States Computer Emergency Readiness Team (US-CERT) reporting requirements
Design and engineering	AT&T will provide all design and implementation services. This will enable the Agency and AT&T to discuss matters such as system recommendations, a baseline assessment, rules, signature sets, configurations, and escalation procedures.

SERVICE DELIVERY APPROACH	TECHNICAL DESCRIPTION
Hardware and software	AT&T will provide intrusion=detection software and hardware components to include sensors, tap, and switches, as applicable.
Implementation	AT&T will provide installation support to include testing of IDPS equipment, testing of software, and loading of any Agency relevant data, as required by the Agency
Multiple layers of protection	MIDS and IDPS are not intended as a single-layer security protection mechanism. Instead, the offers are designed to support additional security services, such as: firewall traffic control, secure routing and networking, secure host computing, and emerging Internet service provider (ISP) network security protection capabilities.
Fully managed solution	AT&T will provide 24x7 management of all IDPS equipment and software. This will consist of monitoring, fault, performance, configuration, and asset management.
Maintenance	Agencies receive equipment hardware and software maintenance that includes updates and replacement. Scheduled maintenance activities are conducted [redacted] In the event that emergency unscheduled maintenance activities are required, AT&T follows pre-established notification procedures to verify notification.
Web-based reporting	Web access to logs and service information
Integrated with other security services	Designed to fully integrate with AT&T's managed firewall solution to provide a robust defense-in-depth security posture for Agency's networks.

Table 1.6.3.1-1: IDPS Service Approach. *L2 and L3 provide the Agency with a comprehensive set of flexible features that will be tailored to meet the Agency's IDS requirements across diverse and complex network environments.*

AT&T's commitment to security is unparalleled. We aggressively research and invest in the technologies and infrastructures required to provide leading-edge security for all aspects of our own network as well as those of our customers. We continually evaluate the changing nature of security needs and continually evolve and expand our security services to meet those needs.

Gartner

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

-- Gartner's North American Managed Security Service Provider (MSSP) Magic Quadrant

AT&T leads the industry in research and development. AT&T Labs on average submits more than a patent a day for technology innovations. As a result AT&T has the technologies and methodologies required to meet Agency's emerging and future security needs.

1.6.3.1.b Benefits to Technical Approach

(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).

AT&T's Networx services, in general, and IDPS services, in particular, support the Government's vision of transformation through the use of the Federal Enterprise Architecture (FEA) by providing the technologies that contribute to the Agency's mission objectives. **Table 1.6.3.1-2** describes each service in relation to FEA, summarizes its contribution, and/or provides an example of how it facilitates FEA implementation.

SERVICE DELIVERY APPROACH	BENEFITS	FEA FACILITATION
Support for standards	Ensures delivery of a service that is consistent with the established best practices, standards and requirements.	Supports the Federal Enterprise Architecture's (FEA's) SPP for Agencies to incorporate security and privacy requirements and services into their EA development lifecycle. In particular: • Service Access and Delivery • *Service Transport* – Supports network services • Component Framework • *Security* - Supports security services
Design and engineering	The design and engineering of IDPS will provide the Agency with a robust level of protection against malicious attacks that could jeopardize mission critical systems.	
Hardware and software	The Agency benefits from the implementation of state-of-the hardware and software that has been rigorously tested in the lab and in operational environments.	
Implementation	AT&T will provide the Agency with all standard pre and post implementation and integration services to ensure maximum operational readiness.	
Fully managed service	Agency benefits from high quality and field-tested IDPS solution that provides real-time 24x7 detection and prevention of security threats, vulnerabilities, and anomalies before they pose a serious threat to the Agency's networks.	
Multiple layers of protection	IDPS is fully integrated with a host of AT&T Managed Security Services (MSS) to provide maximum flexibility and accommodate networks of various size and threat management requirements.	
AT&T IDPS advances	Combination of [redacted] and [redacted] [redacted] applications and tools enable AT&T to provide the most comprehensive and advanced IDPS solution available in MSS market.	
Web-based reporting	Web access to logs and service information.	
Integrated with other security services	Designed to fully integrate with AT&T's managed firewall solution to provide a robust defense in-depth security posture for the Agency's networks.	

Table 1.6.3.1-2: IDPS Service Delivery Approach Benefits. *The IDPS solution provides the best detection mechanism, high stability, high reliability, and intrusion detection and prevention functionality.*

AT&T's development of net-centric technologies supports solutions based on service-oriented architecture (SOA), which uses standardized, web-adapted components. Our approach accords with the following criteria:

- 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 provide line-of-sight linkage to mission performance and ultimate accomplishment per the Performance Reference Model (PRM)
- AT&T operates as an innovative partner through Networx to help achieve the vision of the FEA to enhance mission performance.

In addition to the benefits and FEA facilitations cited earlier, AT&T will assist specific departments and Agencies to meet mission and business objectives through a comprehensive IDPS offering.

1.6.3.1.c Major Issue to Service Delivery

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

In transitioning to 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 has 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 or the most complex projects.

Table 1.6.3.1-3 lists the top eight service delivery risks and our mitigation strategy. As with all large, IDPS 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
Business disruption	In our experience, all Agencies are concerned about business disruption when moving to a new service. Adequate planning will minimize this risk.	[redacted]
New devices	Introducing new system components or devices to an existing, stable network environment always poses a risk that the new devices, and the required configuration of those devices, could disrupt or adversely impact network service.	[redacted]
Equipment functionality	It is not uncommon for premises equipment not to live up to manufacturers' claims and fail to deliver functionality that Agency expects.	[redacted]
Jeopardy issues	All large projects encounter jeopardy issues during service delivery differences between quality provider and competitor in how they are handled.	[redacted]
False Positives	Intrusion-detection sensors are prone to generating false positives	[redacted]
Loss of service.	Server and appliance availability can be an issue.	[redacted]
Interference	Updates and upgrades can interfere with Agency's daily schedule.	[redacted]
Untimely administration	Requested changes to system configuration cannot be deployed in a timely fashion.	[redacted]

Table 1.6.3.1-3: Risk Mitigation to Service Delivery. *IDPS will provide Agencies low-risk services through a structured risk mitigation methodology.*

AT&T has taken steps to identify risk and provide risk mitigation associated with delivering intrusion detection and prevention services. 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.

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

1.6.3.2.a Service Quality and Performance

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

Government Agencies will access high quality network that sets the industry quality standards for performance. AT&T meets the performance levels and acceptable quality level (AQL) of key performance indicators (KPIs) for IDPS for routine and critical users, as presented in the RFP and **Table 1.6.3.2-1**.

KPI	USER TYPE	PERFORMANCE STANDARD (LEVEL/THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
Grade of Service (GoS) (Configuration/Change)	Routine	Within 5 hr of normal priority change	[redacted]
		Within 2 hr for urgent priority change	[redacted]
Event Notification (EN)	Routine	Within 24 hr of low category event	[redacted]
		Within 10 min of high category event	[redacted]
Availability	Routine	99.5%	[redacted]
Time to Restore (TTR)	Without Dispatch	4 hr	[redacted]
	With Dispatch	8 hr	[redacted]

Table 1.6.3.2-1: Security Services Performance Requirements. *The Agency receives high performance services through security operations center.*

AT&T understands the importance of providing as much pertinent information as possible when managing *Networx* IDPS sensors. AT&T's managed security services are based on the requirements outlined in the RFP. AT&T's security event-monitoring system has been selected as the primary interface for managing security events and reporting on them.

The security-event monitoring system provides the information necessary to prove the value of AT&T's security management initiatives through documented resource and team effectiveness. Additionally, it helps the system pass audits and meet internal security Service Level Agreements (SLAs).

THE WALL STREET JOURNAL. *Cyber Security is Hot Niche—AT&T has established an early lead.*

1.6.3.2.b Approach to Monitoring and Measuring Performance

(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.

AT&T monitors key performance indicators (KPIs) to verify that services are within the guidelines of the AQLs within our [redacted] that employs our [redacted] AT&T will accurately measure server availability as calculated by the formula specified in RFP section 2.10.2.4.1 (note 1) and time to restore (TTR) and/or repair. AT&T also benchmarks our performance against industry-wide standards to continually improve on service to our clients. **Table 1.6.3.2-2** provides a description of the approach to monitoring and measuring of the KPIs, as listed by the Government.

KEY PERFORMANCE INDICATOR	MEASUREMENT DESCRIPTION
Grade of Service (GoS) (configuration/ change)	[redacted]
Event Notification (EN)	[redacted]
IDPS Availability	[redacted]

KEY PERFORMANCE INDICATOR	MEASUREMENT DESCRIPTION
	[redacted]
Time to Restore (TTR)	[redacted]

Table 1.6.3.2-2: Monitoring and Measuring Approach. *AT&T has the tools to measure and report compliance with IDPS AQLs and provides additional reporting for threats and threat analysis.*

Of equal importance to identifying the KPIs for a service is the method by which the KPIs are captured, measured, and monitored. Agencies will receive the most accurate assessment of the service when the KPI measurement and monitoring methodology replicates the real performance that Agency personnel experience.

1.6.3.2.c Approach to Perform Service Delivery Verification

(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.

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. **Table 1.6.3.2-3** summarizes the verification and testing procedures for the IDPS KPIs.

KPI	VERIFICATION APPROACH	VERIFICATION/TESTING PROCEDURES
GoS (Configuration/ Change)	AT&T uses a trouble ticket system for tracking changes.	[redacted]
EN	AT&T's security event monitoring system has been selected as the primary interface for managing security events and reporting on them.	[redacted]
Availability	AT&T provides 24x7 monitoring and callout, as needed, of critical application processes. [redacted]	[redacted]

KPI	VERIFICATION APPROACH	VERIFICATION/TESTING PROCEDURES
		[redacted]
TTR	AT&T maintains service agreements with the hardware/software vendors to provide rapid restoration of service in the event of a hardware failure. AT&T also designs the Agency-specific devices with redundancy in mind, so that most hardware failures are repairable with little or no impact to the Agency.	[redacted]

Table 1.6.3.2-3: Verification of Acceptable Performance for IDPS. *AT&T verifies that IDPS consistently operates above the AQL thresholds and that corrective measures are taken expeditiously in the event that these thresholds are missed.*

[redacted]

Through a comprehensive verification process, Agencies and the GSA will receive concrete data that demonstrates the readiness of IDPS. AT&T follows detailed procedures to verify IDPS, by comparing the KPI data against the stated AQLs, as described in the Verification Test Plan and in Section 1.3.2.d Approach to Perform Service Delivery Verification.

1.6.3.2.d Performance Level Improvements

(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.

Achieving the Acceptable Quality Levels defined by the Government for the Key Performance Indicators will result in superior IDPS Service performance. [redacted]

1.6.3.2.e Approach and Benefits for Additional Performance Metrics

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

The KPIs defined by the Government for the Intrusion Detection and Prevention Service (IDPS) will provide a comprehensive assessment for service verification and service performance monitoring. Additionally, we understand the importance of Agencies needing more comprehensive KPIs and on a task-order basis. [redacted]

1.6.3.3 Satisfaction of Security Services Specifications [L.34.1.6.3]

1.6.3.3.a Service Requirements Description

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

1.6.3.3.a.1 Overview

> Stratecast Partners
>
> *AT&T receives the "2005 Best-in-Class NSP Managed Security Services Award" for being "best positioned to serve the broadest and largest number of customers and create strategic differentiation for the company … in the evolving communications industry."*
>
> --April 2005

AT&T will provide the Government an IDPS that is fully compliant with the requirements contained in the Networx RFP and provides the following capabilities: 1) reduces network service disruptions caused by malicious attacks; 2) monitors and identifies potential security threats; 3) detects signs of intrusion that may jeopardize the confidentiality, integrity, availability, and control of Agency networks; 4) uses intrusion sensors to analyze packet activity for indications of network attack, misuse, and anomalies; 5) generates alerts and records suspicious events; and 6) launches immediate corrective responses that stop or alleviate malicious attacks. The following sections present an understanding of the standards, connectivity needs (interfaces), and required technical capabilities related to providing IDPS, as requested in the RFP.

1.6.3.3.a.2 Capabilities and Features

IDPS is a suite of network security tools deployed for both internal and commercial applications. These tools incorporate both system-based and network-based sensing technology, with metadata storage, and advanced data mining and analysis features to detect cyber attacks. They defend very large-scale IP network infrastructures but can be scaled up or down to fit almost any network architecture. **Table 1.6.3.3-1** illustrates the features and capabilities of our IDPS.

CAPABILITIES	TECHNICAL DESCRIPTION
Baseline assessment and network scanning services	Incorporated in every new AT&T IDPS implementation and turn-up. This [redacted] is critical for risk posture analysis and providing correct placement of IDPS sensors. Scanning must be continued throughout lifecycle of security products to continuously re-evaluate customer's security profile and needs.
Perimeter intrusion detection	Continually monitors network traffic for potential misuse or security policy violations. While firewalls typically examine the header of an IP packet and evaluate the specific service being used, AT&T IDPS actually looks into [redacted], and determines its intent, [redacted] The signature database is continually updated as computer security organizations develop new signatures.
AT&T IDPS	Advances in intrusion detection have increased the capabilities of IDS devices; they are now considered a critical piece of an in-depth security portfolio. AT&T's advanced IDPS service provides the following capabilities: [redacted]
Real-time threat management	• AT&T security analysts respond to events in real-time with advanced tools and utilities that enable rapid collection and analysis of security event data collected from vast array of security devices, applications, and operating system environment. • The system also *maintains state* to effectively monitor and manage hundreds of signatures. *Maintaining state* refers to the ability to remember what has happened and compare this with past and current sessions.
Incident response and corrective action	• Immediately upon unauthorized or malicious activities being detected, [redacted] • Upon recognizing patterns of misuse, [redacted]
Implementation and profiling	Creating baseline of knowledge about network traffic patterns and expected noise levels for each deployed sensor: • Sensor deployment at customer-defined sites • Perimeter and internal network implementations • Network and host-based sensors available • Initial profiling and tuning
Time-based attack recognition	Sensors strategically located throughout network search for signatures indicative of hacking attacks or other security violations. Sensors look at content and context of data stream by using blend of pattern matching, stateful pattern matching, protocol decodes, and heuristic-based signatures.
Incident management and analysis	AT&T's IDPS solution increases operational productivity to thwart attacks by: • Reducing time required to analyze log data • Optimizing staffing by automating alert assessments (cutting hours of investigative time) • Increasing accuracy of isolating and responding to attack • Integrating web-based incident management, which provides multilevel escalation and

CAPABILITIES	TECHNICAL DESCRIPTION
	assignment of incidents • Visualizing related alerts across diverse computing architecture to quickly isolate attack • Integrating investigative tools to accelerate incident resolution and features integration with following: [redacted]
Alarm processing, coloration, and response	IDPS uses custom profiling/tuning scheme to examine log and alarm information, correlation, and analysis for vigilant 24x7x365 expert monitoring of all sensors: • Centralized passive monitoring and analysis of alarm streams • Advanced analysis of all alarm activity • False positives eliminated before customer notification • Immediate live customer collaboration in event of severe security incident.
Defense in-depth protection	AT&T IDS is fully managed, comprehensive, IP network attack recognition and response solution for network security. It is premise-based hardware/software solution with AT&T providing hardware components and continuous 24x7x365 support through [redacted] By leveraging AT&T IDPS solution, Agency takes advantage of AT&T's unparalleled security experience and expertise, which is directly derived from managing and securing global IP network.
Online reports	Reports are available on Business Direct by subscribing to the "View Your Managed Security Reports" tool. List of Reports available: • IDS Severity Summary Report • IDS Directions & Severities • IDS Top 20 Events by Destination IP Address • IDS Top 20 Events by Service • IDS Top 20 Events by Signature • IDS Top 20 Events by Source IP Addresses • Trouble tickets

Table 1.6.3.3-1: Agency-Derived Benefits from IDPS Solution. *IDPS offers Agencies the fully managed IDPS solution that provides real-time event detection and analysis capabilities.*

The AT&T SNOC's responsibility encompasses management of alarm detection, notification of security breaches to customers, analysis of attack data, interpretation of attacks, and forensics. The AT&T SNOC provides intrusion detection service monitoring wherever a sensor is placed throughout the customer's network. The AT&T SNOC takes the appropriate predefined action based on alarm conditions to resolve the arising intrusions. The IDPS management system is located at the AT&T SNOC where it is in constant communication with the IDS sensors and provides visibility into the perimeter security of a client network. The Management System controls the configurations of each [redacted]-secure IDS sensor and will deploy signature updates to the sensors [redacted]. When an alarm is activated by the management system, a trouble ticket is generated, and AT&T security professionals respond immediately. The generation of an alarm is critical and triggers an automated or manual response to the attack. This response mitigates the potential damage of the specific event.

1.6.3.3.a.3 Interfaces

In accordance with the RFP, the IDPS connects and interoperates with following connectivity interfaces **Table 1.6.3.3-2**.

Underlying Networx Offering	IDPS Supported
Internet Protocol Service (IPS)	✓
Premises-Based IP VPN Services (PBIP-VPNS)	✓
Network-Based IP VPN Services (NBIP-VPNS)	✓

Table 1.6.3.3-2. Transport Services available for IDPS: *Available to the Agencies are a variety of transport service options to support IDPS.*

1.6.3.3.b Attributes and Values of Service Enhancements

(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.

In addition to the standard features described above, Agencies can enhance their IDPS with additional features and capabilities. **Table 1.6.3.3-3** highlights additional service features and capabilities available with IDPS.

Service Enhancement	Description	Benefit
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 1.6.3.3-3: Service Enharnachements. *Agencies will receive additional reporting and signature services as part of our standard service offering.*

1.6.3.3.c Service Delivery Network Modifications

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

The KPIs defined by the Government for the IDPS will provide a comprehensive assessment for service verification and service performance monitoring. [redacted]

1.6.3.3.d Security Services Experience

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

AT&T Networx Team offers Agencies extensive experience providing managed services that create value to our customers to both in Government and commercial entities. This experience has given us the ability to engineer and deliver services. Two examples of AT&T Team's ability to deliver managed services are listed in **Table 1.6.3.3-4**.

	[redacted]	
Client Need	*Solution*	*Created Value*
[redacted]	[redacted]	[redacted]
	[redacted]	
[redacted]	[redacted]	[redacted]

Table 1.6.3.3-4: Service Experience. *AT&T has an extensive history of providing IDPS services to customers.*

AT&T has deployed IDP solutions to its own infrastructure, as well as protecting large customers. This and other industry experience is described in **Table 1.6.3.3-5**.

EXPERIENCE	DESCRIPTION
AT&T Infrastructure	Guards against malicious code to [redacted] AT&T's IDPS program was initially designed to protect AT&T's vast IP infrastructure, which is universally regarded as the largest and most comprehensive IP network in the world today.

EXPERIENCE	DESCRIPTION
Industry Leadership	AT&T is actively involved in a wide range of security initiatives, from the Chief Executive Officer (CEO) level (providing direct support to the Office of Homeland Security) to the many forums, councils, associations, and committees on which various AT&T executives, scientists, and professionals serve. For many years, AT&T has led the information security industry in designing, developing, and deploying security solutions. Our industry leadership spans the spectrum from authoring books on security topics to the extensive involvement of AT&T representatives in forums, working groups, and associations involved in various security initiatives.
Staff Experience	AT&T staffs one of the largest security organizations in private industry, with over [redacted] professionals who possess a wide variety of advanced technical and managerial degrees, PhDs, and industry-recognized security certifications. This vast talent pool enables AT&T to provide the Agencies with an unparalleled level of expertise and support.
Industry forums	Our security professional's work with a wide variety of Government and civilian forums to address some of the most pressing security concerns in the U.S. AT&T is also involved in supporting various other security-related initiatives. These examples demonstrate our commitment to security at all levels and from all aspects: • 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) • National Security Telecommunications Advisory Committee (NSTAC) • AT&T is a leader in the Internet Engineering Task Force (IETF) security efforts.

Table 1.6.3.3-5: Service Experience. *AT&T has an extensive history of providing IDPS services to protect our own vast infrastructure.*

1.6.3.4 Stipulated Deviations

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

1.6.3.5 EMNS Intrusion Detection and Prevention Service (IDPS)

The added sections are provided to Agencies ordering Enhanced Managed Network Service (EMNS) and are ordered with other EMNS service components.

1.6.3.5.1 EMNS IDPS - Service Description

The Enhanced Managed Network Service IDPS is a [redacted] IDPS solution. The EMNS IDPS provides comprehensive inspection process for data protection and integrity while optimizing performance and reducing risk.

The IDPS functionality at the [redacted] uses appliances from [redacted]. The [redacted] Intrusion Protection System integrates application and network visibility with incident investigation and remediation. AT&T's

evaluation showed the [redacted] IPS was the best such device among market leaders considered.

Figure 1.6.3.5-1 shows that the [redacted] IPS defends against a wide range of attacks such as: Stateful Signatures, Protocol Anomaly, Backdoor Detection, Traffic Anomaly, Network Honeypot, DOS Detection, Spoofing Detection and Compound Signatures. The solution's security mechanism stops network attacks on the EMNS solution with the IPS's wide range of incident support. We forward incident reports from our NOC/SOC to the Government's SOC.

Figure 1.6.3.5-1: EMNS IDPS Service. *The EMNS Intrusion Detection and Prevention Service provides thorough and complete IDS packet inspection process using state of the art technology while allowing for future service applications.*

AT&T uses a centralized management station to manage the [redacted] IPS appliances. The management station allows the Agency to view all logs and alerts including those stored for historical data mining for up to [redacted] years.

When directed by the Agency, AT&T will monitor inbound and outbound traffic at selected EMNS sites using IDPS technologies that provide for the detection of signature, anomaly, and behavior events or use any other Agency approved detection method within the client site.

Table1.6.3.5-1 describes the peak port speeds for the EMNS IDPS service:

DESCRIPTION
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

Table 1.6.3.5-1: EMNS [redacted] IDPS Port Speeds. *The EMNS Node-based IDPS provides peak ports speeds that range from* [redacted]

1.6.3.5.2 EMNS IDPS – EMNS IDPS Enhanced SED (ESED) Description

For the EMNS IDPS service, the [redacted] Intrusion Prevention System (IPS) will be provided EMNS IDPS ESED. The [redacted] IPS solutions accurately identify, classify, and stop malicious traffic, including worms, spyware, adware, network viruses, and application abuse, before they affect Agency continuity of operations.

One of the following Cisco IPS sensors will be bundled with the EMNS IDPS offering:

[redacted]

[redacted]

In addition to providing a [redacted] IPS Sensor at each EMNS IDPS location, the following ancillary site services are included with the EMNS IDPS ESED.

- Equipment and accessories required to install and maintain the EMNS IDPS ESEDs at all EMNS IDPS sites. This shall include, but is not limited to, racks, cables, tools, etc.
- Space and power requirements - such as physical space, rack space, power, and HVAC - defined for EMNS IDPS ESED at each EMNS IDPS site.
- Operations and management of hardware and software components up to the EMNS IDPS demarcation point.

AT&T will label and run cable according to guidelines provided by the Government in locations where cable extensions are required to connect an EMNS IDPS ESED to the Government-specified demarcation point. Government guidelines and any additional local procedures provided by the Government will be followed for accessing, installing and maintaining all EMNS IDPS ESEDs.

The Installation and Maintenance CLINs for the EMNS IDPS ESEDs will be found in section B.4.11 of the Pricing Volume.