1.6.4 Vulnerability Scanning Service (VSS) [C.2.10.3]

Vulnerability scanning is a major component of risk assessments, aiding Agencies in complying with Federal requirements to conduct periodic risk assessments of their security controls. Vulnerability Scanning Service (VSS) is a flexible, high-quality solution that reduces the total cost of ownership (TCO) of protecting Agency infrastructure and critical assets.

VSS works in line with security policies to perform network discovery and prioritization, vulnerability assessment, risk rating, threat correlation, asset-based remediation management, and measurement and reporting.

AT&T uses a reliable automated process [redacted] with [redacted] yields optimal results, enabling VSS to provide effective security protection against threats or malpractices that may negatively impact operations.

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

1.6.4.1.a Approach to Service Delivery

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

Vulnerabilities can be exploited directly by an attacker, or indirectly through automated attacks, such as Distributed Denial of Service (DDOS) or computer viruses. Statistics show that 95 percent of all security breaches result from known vulnerabilities and mis-configuration[1]. Federal agencies, security software vendors, security consulting firms, and incident response teams collaborate to discover, track, and mitigate vulnerabilities. Specialized databases such as the

Source: 2004 E-Crime Survey; CSO Magazine; CERT [redacted] and [redacted] have been created specifically for reporting vulnerabilities and associated resolution.

Customer requirements dictate the design, deployment, configuration, and management of VSS. VSS can be deployed in dedicated or hosted environments with customer-managed or AT&T-managed options. Irrespective of the option chosen, VSS allows agencies to take control of the vulnerability management life cycle by discovering potential vulnerabilities in their networks and determining the best actions to prevent potential attacks from succeeding.

This service analyzes Agencies' operating systems, networks, commercial off-the-shelf and custom applications, and wireless devices, to uncover potential security breaches. The scanning service is available 24x7 for internal and external scans. **Figure 1.6.4.1-1** shows the three major system components, potential architectures, and service features of VSS.

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 Services], is awarded the Customer Solutions Excellence Award."*
>
> --Frost & Sullivan
> July 2003.

AT&T uses [redacted] products for VSS. Founded in 1999; [redacted] is a pre-eminent leader in security solutions, serving hundreds of high profile organizations in the Fortune 500, Federal and state governments, and the military. [redacted] award-winning products help protect the networks of many of the world's most-at-risk organizations. The main components of this service are the [redacted], VSS database, and scan engine.

Figure 1.6.4.1-1: VSS Architecture Using [redacted] Solution. *Agencies will mitigate risk of vulnerabilities by carefully balancing asset value, vulnerability severity, and threat criticality.*

The [redacted] is a web portal that provides a centralized view of the entire vulnerability management process: asset discovery, prioritization, monitoring, remediation, and reporting. The scanning engine enables asset discovery and vulnerability analysis across the Enterprise with unprecedented management and control. The VSS database is a repository that integrates Agency-specific data with [redacted] knowledge base built from years of experience. All VSS components will be scaled accordingly to the size and complexity of the network. [redacted] AT&T also supports a fully hosted solution, for which all equipment resides outside the customer premise in our Internet Data Center (IDC). Our IDC provides logical and physical separation for additional security. The IDC also hosts dedicated and shared infrastructures. Some of our service support features include notifying customers via email, pager, fax, or telephone; assisting with corrective actions; scheduling scans, and web access. Customers dictate their involvement in performing the actual scans, managing, and maintaining the infrastructure. VSS is even available to customers that use other Internet Service Providers (ISPs).

VSS will support Agency needs to continue daily operations without loss of productivity. Existing network vulnerabilities can be exploited to compromise the confidentiality, integrity, and availability of data or the possible loss of valued assets. VSS accurately identifies issues and alerts Agencies of existing-weaknesses and potential countermeasures. In summary, the service will be integrated into our customers' overall security architecture, accommodating networks of varying size and complexity. **Table 1.6.4.1-1** highlights our approach to service delivery.

Service Delivery Approach	Technical Description
Robust scanning capabilities	Conducts deep infrastructure probes, beginning with less intrusive checks and escalating in sophistication across [redacted] IP addresses. Executes scanning at unmatched speeds (Class C in [redacted] Class B in [redacted] Class [redacted] [redacted] IPs in [redacted]).
Reliable performance	• [redacted] award-winning technology provides highest accuracy rate in the marketplace. Accuracy is achieved by using a combination of the following factors: • Effective OS identification • Matching vulnerability checks to target systems' OS, open services, as well as the network service protocol (i.e., UDP/TCP) • Disciplined creation/development of vulnerability checks • Rigorous quality assurance • Responsive technical support • [redacted] reliability combined with AT&T security consultant expertise yields unmatched VSS performance.
Scalable architecture	• Scales to address most complex globally distributed IT infrastructures. AT&T supports both, AT&T hosted and customer premised-based architectures. • **AT&T Hosted Architecture:** • Ideal for customers lacking the space, capacity, or expertise for maintaining equipment and functionality of VSS. • Devices placed inside AT&T IDCs • 24x7 management and monitoring • Customers have the option to use shared or dedicated infrastructure • Variety of management/service options available [redacted]
Standards compliance	• VSS complies with all Federal regulations 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 199 — Standards for Security Categorization of Federal Information and Information Systems

	• NIST Special Publication (SP) 800-51 — Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme • United States Computer Emergency Readiness Team (US-CERT) reporting requirements
Easy and convenient access	• Web-based secured access via [redacted]. • Supports AT&T and third-party access methods. • Customers have access to configurations and reports.
Value and support	• VSS creates efficiencies and scales to large enterprises to drive down the total cost of ownership. • AT&T technical security team is available 24x7 and provides leading customer service. • AT&T managed customers receive notifications/alerts, assistance with corrective actions, scan scheduling, and web access.

Table 1.6.4.1-1: VSS Delivery Approach Summary. *The Agency will realize its vision for VSS through the deployment of a comprehensive service that will be configured to suit different environments – from a small LAN to the largest, most complex network.*

VSS is a security solution that will continuously and reliably assesses network assets for vulnerabilities and then provide effective reporting to allow a security team to remediate these liabilities. VSS uses a priority-based approach to risk management to help Agencies mitigate risk and carefully balance asset value, vulnerability severity, and threat criticality.

AT&T recognizes that enterprise resources are limited, so by focusing on the most important assets, vulnerabilities, and threats first, an Agency can direct resources where they will have the greatest return in improving the security health of the organization. The VSS asset criticality labeling, security metrics, and other intuitive reporting features measure the risk posture and communicate improvements, based on decisions the Agency makes.

> Gartner *Gartner Rates AT&T highest in 'Ability to Execute' as a Managed Security Service Provider.*
>
> —Gartner's North American Managed Security Service Provider (MSSP) Magic Quadrant
>
> February 2003.

1.6.4.1.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 VSS offering supports the Government's vision of transformation through Federal Enterprise Architecture (FEA) as a facilitating mechanism for technologies that contribute to mission performance. AT&T is aligning its componentized products and services so they are easily integrated, manageable, seamlessly available across platforms, and usable across Government functions—both horizontally and vertically—as well as between levels of Government. **Table 1.6.4.1-2** outlines the benefits and features that contribute to FEA and Agency objectives.

SERVICE DELIVERY APPROACH	BENEFITS	FEA FACILITATION
Robust scanning capabilities	• Increases operational efficiency of risk identification, tracking, and mitigation by being able to run scheduled/unmonitored scans and can scan [redacted] IP addresses on weekly basis by automation	Supports FEA's SPP for Agencies to incorporate security and privacy requirements and services into their enterprise architecture development lifecycle. In particular: • Service Access and Delivery *Service Transport* – Supports network services • Component Framework *Security* - Supports security services
Fast performance	• Provides continuous service so that the network is constantly rediscovered and analyzed, which drastically reduces the time interval between the introduction and discovery of vulnerabilities, allowing the Agency to discover and correct their vulnerabilities in the shortest amount of time.	
Scalable architecture	• Scales to accommodate networks of varying sizes and complexity [redacted] • Investment in VSS solution can grow as business requirements grow, supporting FEA requirements to support cross-agency initiatives, leverage technology, and reduce redundancy where overlap limits value of IT investments.	
	• AT&T Hosted Architecture: Ideal for customers lacking the space or expertise for maintaining equipment and functionality of VSS. Devices placed inside [redacted] and monitoring. Customers have the option to use shared or dedicated infrastructure. Variety of management/service options available	
	• [redacted] - Cost-effective solution for a smaller Agency because it [redacted]	
	• [redacted] - For a larger network, the Agency benefits from this option by [redacted] This configuration allows a greater number of devices to be scanned	
	• [redacted] - For multiple networks, the Agency benefits from this solution, which is an extension of the [redacted], by allowing the scanning to be [redacted], thus permitting scanning of many networks simultaneously.	
Effective processing	Allows vulnerabilities to be discovered, reported to owning teams, and corrected faster.	
Standards compliance	Delivery of a service that is consistent with established industry best practices	

Table 1.6.4.1-2: Agency Derived Benefits from VSS Security Solution. *VSS offers the Agency a vulnerability scanning solution that has a flexible, scalable architecture offering cost-effective, risk mitigation compatible with the FEA.*

VSS is part of our overall security strategy, which includes providing a multilayered security environment, designing security into the network and services, focusing on methods and systems to enhance security, and responding to and mitigating incidents. The multilayered security approach is extended by transferring our own proven security innovations to the Agency.

1.6.4.1.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 task-based or fully outsourced, unforeseen issues are inevitable. 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 from the simplest to the most complex projects.

AT&T has taken steps to identify risk and provide mitigation associated with delivering VSS. **Table 1.6.4.1-3** lists the top ten service delivery risks and our mitigation strategy. As with all large, vulnerability scanning 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
Service delivery	All large projects encounter jeopardy issues during service delivery differences between quality provider and competitor in how they are handled.	[redacted]
Untimely administration	Updates and upgrades can interfere with Agency's daily schedule. Also, requested changes to system configuration cannot be deployed in a timely fashion.	[redacted]

		[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]
Intrusive scans may cause DoS, brute force, and other attacks.	VSS offers users the option of running non-intrusive vulnerability checks and/or intrusive checks that mimic the actual attack for an extremely accurate assessment. Checks labeled as non-intrusive in the VSS database are designed to work without any possibility of service disruption and with minimal impact on the target systems.	[redacted]
Unauthorized or risky ports left open	Scanning may require the opening of some ports that would otherwise be closed or not allowed to transverse the firewall during normal business operations.	[redacted]
Inaccurate results	Scan results may sometimes return or produce false positives or negatives, depending on unique system configuration. For example, a scan result may provide the incorrect OS and patch version for a particular system.	[redacted]
Introduction of new device(s) into the network	VSS requires the placement and operation of new devices in the network, which may introduce a possible risk to Agency architecture should VSS devices be compromised or not be able to successfully interact with other existing devices.	[redacted]
Business disruption during turn-up.	In our experience, all Agencies are concerned about business disruption when moving to a new service. Adequate	[redacted]

	planning will minimize this risk.	[redacted]
Sizing	Often, when scanning many packets on very large enterprises, antivirus clusters can become overwhelmed and impede performance.	[redacted]
Loss of service.	Network, OS, or any other technical issues may cause the VSS Server and appliance to be unavailable.	[redacted]

Table 1.6.4.1-3: Risk Mitigation to Service Delivery. *VSS will provide reliable service, allowing the Agency to concentrate on core business issues.*

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.

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

1.6.4.2.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.

AT&T is committed to offering high quality in security service. This commitment extends beyond simple promises. Our commitment is supported by offering the Government financial commitments in the form of Service Level Agreements (SLA). AT&T will meet the performance levels and acceptable quality level (AQL) of key performance indicators (KPIs) for VSS for routine and critical users, as presented in the RFP and in **Table 1.6.4.2-1**.

THE WALL STREET JOURNAL.

Cyber-Security is Hot Niche - AT&T has established an early lead.

Government Agencies will access the highest quality network offered that sets the industry quality standards for performance.

KEY PERFORMANCE INDICATOR	USER TYPE	PERFORMANCE STANDARD (THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
VSS Availability	Routine	99.5%	[redacted]
Time to Restore (TTR)	Without Dispatch	4 hr	[redacted]
Time to Restore	With Dispatch	8 hr	[redacted]

Table 1.6.4.2-1: Performance Metrics for VSS. *AT&T's performance for vulnerability scanning service meets or exceeds performance metrics, providing operational continuity on a 24x7 basis.*

AT&T's confidence in our ability to deliver these performance results is supported by past performance and is backed by stringent service credits.

1.6.4.2.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 the KPIs to verify they are within the guidelines of the AQLs within our Security Operations Center (SOC) using our automated [redacted] AT&T will accurately measure server availability and time to restore (TTR) and/or repair. AT&T also benchmarks our performance against industrywide standards to continually improve on service to our clients. **Table 1.6.4.2-2** provides a description of the approach to monitoring and measuring the KPIs.

KEY PERFORMANCE INDICATOR	MEASUREMENT DESCRIPTION
VSS Availability	[redacted]
Time To Restore (TTR)	[redacted]

Table 1.6.4.2-2: Monitoring and Measuring Approach. *AT&T has the tools to measure and report compliance with VSSW AQLs.*

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. To provide the Agencies with the most accurate representation of the service performance, AT&T has deployed a separate performance measurement infrastructure to collect network performance information. AT&T's measurement methodology, therefore, more closely captures the real performance that end users experience by measuring the data path that is very similar to the paths that the end user data would follow.

1.6.4.2.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.

AT&T will conduct monthly service quality reviews with the Agency to discuss AT&T's performance, including adherence to contracted performance guarantees. **Table 1.6.4.2-3** 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 are monitored to certify that the service performance complies with the AQL.

KPI	Verification Approach	Verification/Testing Procedures
VSS Availability	[redacted]	AT&T will track service outage from time trouble ticket is opened until the problem is repaired.
Time To Restore (TTR)	[redacted]	Trouble tickets are analyzed and TTR statistics are updated and compared with targets.

Table 1.6.4.2-3: Verification of Acceptable Performance for VSS. Measures *VSS to assess consistent operation at or above the AQL thresholds, and that corrective measures are taken expeditiously in the event that these thresholds are missed.*

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 AT&T [redacted] 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.

1.6.4.2.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 (AQL) defined by the Government for the Key Performance Indicators will result in superior VSS performance. AT&T is open to negotiate AQL values with Agencies on a task-order basis.

1.6.4.2.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 VSS provide a comprehensive assessment for service verification and service performance monitoring. However, we understand the importance of Agencies needing more comprehensive KPIs. On a task order basis, therefore, AT&T will analyze the Agencies' enterprise architecture business objectives and develop more comprehensive KPIs and AQLs.

1.6.4.3 Satisfaction of Security Services Specifications [L.34.1.6.3]

1.6.4.3.a Service Requirements Description

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

The following sections present an understanding of the technical capabilities, features, and interfaces related to VSS.

1.6.4.3.a.1 Capabilities

Host discovery, service detection (on standard and nonstandard ports), vulnerability assessment, threat-correlation, and remediation management are some of the most comprehensive capabilities of VSS. **Figure 1.6.4.3-1** shows a typical service network configuration, [redacted] The servers use [redacted] data to communicate between servers over [redacted]. All intra-server communication is [redacted] Only one port needs to be allowed in the firewall configuration for a [redacted] to function.

VSS analyzes network devices and applications (through the use of pre-defined standard or customer-defined checks) based on OS, open ports, and protocols. Checks (such as brute force) that may be applicable across various devices/OS types are executed on all targets.

Figure 1.6.4.3-1: VSS Security Solution Back-end Architecture. *Agency vulnerability scanning security needs will be met in a secure, comprehensive manner* [redacted]

By default, AT&T uses non-intrusive checks. Intrusive checks are enabled only at the customer's request. Attacks can vary depending on the vulnerability; so VSS considers many factors (such as speed of check execution, impact on target machine, type of attack, and type of vulnerability). In determining when/if a host is vulnerable, VSS uses assessment modules to uncover weaknesses in various OS types, wireless, web, custom, and other off-the-shelf applications. VSS also uses a ranking or priority system (high, medium, low, and informational) to categorize found vulnerabilities. These categories are based on the likelihood of exploitation and impact to the system. Ranking or prioritizing categories is helpful to agencies in developing a plan of action and milestones for vulnerability mitigation.

VSS will have minimal impact on the network. Although VSS requires approximately [redacted] users have the flexibility to fine tune this requirement against the scanning performance required. Some users choose to scan the entire network in one session while others scan various segments of the network across multiple sessions. Running VSS requires internal coordination with system administrators and other agency staff, as some of the traffic generated may trigger system alerts on perimeter defense devices such as firewalls or intrusion detection systems. For customer-managed options and administration, VSS provides a granular level of access control that incorporates usernames, passwords, user rights, and privileges.

Figure 1.6.4.3-2 shows another example of how the VSS infrastructure is integrated with AT&T and customer networks to manage remote scan engines. By leveraging the customer premise with AT&T infrastructure, AT&T will provide remote scanning that only uses [redacted] between the servers. This minimizes the hardware requirements for the end-user and allows for a centralized storage and correlation of data. [redacted]

[redacted]

Figure 1.6.4.3-2: VSS Security Solution Architecture for External Scans. *This infrastructure design, similar to the internal vulnerability scanning infrastructure, is configured for scans external to the firewall and uses AT&T's infrastructure as part of the architecture.*

In **Figure 1.6.4.3-2**, The VSS database runs on an [redacted] server within the network. It stores such data as scan settings, scan results, remediation tickets, and user account information, providing the information needed to generate reports and run scans. [redacted]

[redacted]

The thoroughness and accuracy of VSS can be modified as customers see fit, allowing for granular control over ports to be scanned, timeouts, inter-packet delays, and the number of times each host discovery sequence is executed. VSS uses [redacted] proprietary OS identification technique [redacted] was created to overcome the limitations of existing fingerprinting techniques and uses only RFC-compliant packets. There is a maximum requirement of one open TCP port and three packets for proper identification. [redacted] was also designed to provide a high degree of accuracy, while still allowing scans to execute quickly with minimal network impact. Many other tools use host discovery techniques require multiple ports to be open on target systems. Often, these other tools inaccurately identify hosts when there are filtering devices between the scanning system and target.

As previously mentioned, the VSS host discovery features will identify any device participating on the network (i.e., bearing an IP address). This technique covers not only a wide range of traditional devices (e.g., servers, routers, and databases), but also nontraditional devices that are also Internet-connected (such as specialized control systems and other customized hardware). The VSS OS identification is equally complete, allowing for OS identification, even when target systems are only available on ICMP.

TCP services are detected either with TCP SYN scanning or with TCP full connect scanning (i.e., complete handshake). UDP scanning will identify services using two techniques: (1) Issuing protocol specific requests for a particular service (i.e., nudge strings) to elicit a specific response from an active service, such as a host name resolution request for DNS, and (2) Noting the absence of ICMP port unreachable messages after having performed an initial test to determine if these messages were ever sent. The combination of these methods allows for highly accurate discovery of UDP, enabling VSS to determine and accommodate the possibility that the remote host is throttling ICMP responses, such as is the case with Linux kernels. The thoroughness and accuracy can be modified as customers see fit, allowing for granular control over ports to be scanned, time-outs, inter-packet delays, and the number of times each service discovery sequence is executed.

1.6.4.3.a.2 Features

VSS offers many unique features which are highlighted in **Table 1.6.4.3-1**.

SERVICE FEATURE	TECHNICAL DESCRIPTION	BENEFITS TO AGENCY
Vulnerability scanning	• Scans all live hosts for known vulnerabilities. Vulnerability assessment tests for most recent vulnerabilities. Results are arranged according to four levels of vulnerability severity – informational, low, medium, and high. VSS associates the common vulnerabilities with: • Backdoors • Bind • Browser • Brute Force Attacks • CGI-BIN • Daemons • Distributed Component Object Mode • eCommerce Applications • Email • Firewalls • Hubs/Routers • Instant Messaging	•Reduction in total cost of ownership •Secure and protect all assets & resources •Business prioritization and drivers •Organization size, structure, goals, and guidelines •Security policy and risk tolerance •Policy and compliance •Vulnerability history and experience •Complete control and visibility into vulnerability management lifecycle
Network Identification and enumeration	VSS can identify any device or range of devices on the network that use IP addresses. Once a device is identified, the next step is enumeration. Enumeration determines attributes such as name, operating system (OS), application versions, and patch level. VSS performs 4 types of ICMP analysis, UDP scanning, and TCP SYN scanning to discover OS, routers,	• Build a map of entire network • Create an inventory or profile for every single device • Determine compliance

	hubs, switches, load balancers, firewalls, printers, mainframes, midrange systems, minicomputers, and many others. Provides logical and graphical map of entire enterprise infrastructure - including servers, databases, load balancers, wireless access points, web applications, and virtually any other machine connected to network. Used for rating criticality of devices where any vulnerabilities are found.	• Uses standard protocols • Supports commercial off-the-shelf or custom applications • Supports legacy applications or devices • Wireless support
Asset management and assessment capabilities	Analyzes the delta between current security procedures and vulnerability management industry best practices through the use of modules, including threat-correlation and remediation.	• Compliance with security requirements • Identifies gaps or trouble areas • Provides potential for attacks • Insight into organizational impact and business disruption
Enhanced remediation	• Provides intuitive means of making asset owners accountable for addressing security weaknesses. • Provides security managers with step-by-step control over fixing vulnerabilities, with automated verification, confirming that vulnerability was actually fixed before allowing ticket to be closed.	• Accountability • Helps build a plan of action • Closes loop for resolution
Measurement and reporting	• VSS delivers secure, automated reports showing results in comprehensive and comprehendible fashion. It also includes detailed attributes of network, as well as identified vulnerabilities and associated countermeasures. • Users interface with the web portal to perform administrative-type functions such as schedule and setup scans, run reports, manage user accounts, access remediation tickets, and track progress at fixing vulnerabilities. • Reports are easy to read and available in a variety of formats and can be integrated with other AT&T services such as Business Direct. • VSS also embeds easy-to-understand metrics to provide customers with effective means of measuring and monitoring security risk to network resources. • Organizations can quickly assess their security posture, benchmark business units or regions, and track progress of implemented security policies and programs.	• Insight into real-time and historical records • Ease of management and maintenance • Web-based system • Easy but secured access • Helps communicate to other technical staff or senior management
Alerting	VSS service options include agency notification, assistance with corrective action, scan scheduling, and web access.	• Keep administrators informed • Various notifications methods available • Opportunity to eliminate vulnerabilities before these are exploited
Modular Architecture	• VSS is equipped with a variety of standard and specialized modules, including general assessment, windows assessment, wireless assessment, web application assessment, threat-correlation, and remediation. • Specialized modules have the capability to perform source-sifting, authentication testing, source-code disclosure, SQL query misuse, and smart guesswork.	• Various architectures to meet requirements • Uses customer-premise • Extends AT&T infrastructure • Communicates via AT&T network • 3rd party access
Continuous analysis	VSS provides continuous service so that network is constantly rediscovered and analyzed, which drastically	• Enable only what is needed

	reduces time interval between introduction and discovery of vulnerabilities.	• Supports custom applications • Various architectures to meet requirements • Uses customer-premise • Extends AT&T infrastructure • Communicates via AT&T network • 3rd party access •
Unparalleled manageability	AT&T managed or customer-managed options	
Automated updates	• Automatic download capability provides an alternative to manual downloads in the event the Internet is not available. VSS maintains an updated database and correlation engine with the latest vulnerabilities.	• Receive the latest vulnerability information with minimal human intervention • Consistent and reliable communication
Enterprise-class	Scales to accommodate networks of varying sizes and complexity [redacted] as shown in Figure 1.6.4.3.A-1. VSS is also used [redacted] t o protect [redacted]	• State-of-the-art equipment • Unmatched, reliable performance • Experienced security professionals • Dedicated service support • Scalable and modular architecture
Interoperability	Leverages existing investments in established technologies and business processes by responding to growing acceptance of vulnerability management as part of overall information technology (IT) and security infrastructure with open, standards-based approach. Supports Application Programming Interface (API) for Window-based applications. Other interfaces can be acquired to integrate Agency's own tools and applications to assist in-house security personnel in their scanning needs. One example would be to use standard extensible markup language (XML) API, as required by Agency.	• Secure current investments • Reduce TCO • Support legacy environments • Uses standards-based approach • In-line with industry best practices • Easy integration

Table 1.6.4.3-1: VSS Capabilities Meets Agency's Vulnerability Scanning Requirements. *The Agency will be provided with a fully managed, high-quality service.*

1.6.4.3.a.3 Interfaces Description

Our service interfaces with Agencies' networks as shown in **Figures 1.6.4.3-1 and 1.6.4.3-2**. Devices can be placed in the agencies' local area network (LAN) or inside an AT&T hosting facility or IDC. All interfaces require an IP address and may interact with other AT&T services such as Internet Protocol Service (IPS), Premises-Based IP VPN Services (PBIP-VPNS), and Network-Based IP VPN Services (NBIP-

"But in the last year and a half they [AT&T] have been bitten by the security bug. They are aggressively evaluating next-generation technology. [AT&T] is a true thought leader in the industry."

--The Yankee Group
June 2003.

VPNS) through the shared gateway perimeter protection.

1.6.4.3.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.

[redacted]

[redacted]

[redacted]

1.6.4.3.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.

Agencies receive a low-risk solution through AT&T's ability to offer VSS upon contract award without modifications to the network or operational support systems.

1.6.4.3.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 has provided VSS to both internal, Government, and commercial entities in the past. This experience has given us the ability to engineer and deliver services that create value to our customers. **Table 1.6.4.3-2** cites some examples of AT&T's ability to deliver VSS.

[redacted]

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

[redacted]

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

[redacted]	[redacted]	[redacted]

Table 1.6.4.3-2: Service Experience. *AT&T has an extensive history in providing vulnerability scanning services to both customers as well as protecting their own vast infrastructure.*

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*

1.6.4.4 Stipulated Deviations

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