6.4 VULNERABILITY SCANNING SERVICE (L.34.1.6)

Through our Vulnerability Scanning Service offering, Qwest allows Agencies to conduct effective and proactive security assessments of critical network and computing components, enabling the rapid correction of vulnerabilities before they are exploited.

Qwest Vulnerability Scanning Service (VSS) is a proven and effective service that meets the requirements of General Services Administration (GSA) and the Agencies. VSS is an online vulnerability management solution that evaluates the security of networks remotely providing for 24x7x365 detection and protection by identifying real-world weaknesses. The Qwest Team has selected Qualys Inc.'s,QualysGuard, to offer an on-demand VSS vulnerability management solution [redacted]

The Qwest Team meets all GSA requirements for service delivery, performance, and service specifications. VSS is a valuable component of the Qwest Team's in-depth defense strategy of Managed Tiered Security Services (MTSS). An Agency may choose VSS alone or in combination with other services. Qwest VSS includes:

- A comprehensive, on-demand security audit that identifies, analyzes, and reports on security threats to Agency systems, networks, and applications
- A knowledge base of exploits that is updated daily from information provided through strategic relationships and a skilled staff of dedicated security engineers
- Scanning and auditing of the majority of commercial and open source applications on more than 200 different platforms and operating systems

Data contained on this page is subject to the restrictions on the title page of this proposal.

- Performing external scans by remotely probing a network for vulnerabilities that are exploitable from the Internet
- Performing internal scans using a scanner appliance that detects flaws that are exploitable from the inside of networks

These features make the Qwest VSS an excellent choice for GSA and the Agencies.

6.4.1 Technical Approach to Vulnerability Scanning Services Delivery (L.34.1.6.1)

The Qwest technical approach for VSS is to incorporate an on-demand, service-based vulnerability management solution through a trusted third-party operating at a Security Operations Center (SOC) as opposed to acquiring, installing, supporting, and maintaining an in-house product-based solution [redacted]

6.4.1.1 Approach to Vulnerablity Scanning Service Delivery (L.34.1.6.1(a))

Qwest's VSS solution meets all Networx service delivery requirements and can be immediately deployed. With Qwest's VSS, the Qwest Team provides Agencies with the capability to perform effective and proactive assessments of public and private networks, while applying rapid correction of vulnerabilities before they are exploited. Qwest's engineers will analyze

Data contained on this page is subject to the restrictions on the title page of this proposal.

each Agency's specific requirements to configure VSS using Qwest's solution.

Qwest's VSS functions are achieved through technology, proven processes, and a trained and skilled security engineering team. Qwest's VSS has the ability to perform [redacted]

Qwest's VSS fulfills all the mandatory requirements for VSS capabilities, including Key Performance Indicators (KPIs)/Acceptable Quality Levels (AQLs), standards and interfaces, vulnerability detection, features, processes, Agency customization options, and benefits listed below.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

Qwest's VSS is compatible with all security standards required in the Request for Proposal (RFP), including FISMA, NIST (SP) 800-51, FIPS 199, etc. Qwest's VSS is certified as Common Vulnerabilities and Exposures (CVE) approved by Mitre. It has CVE or CAN numbers listed for all applicable vulnerabilities and maintains a 6-Sigma software quality rate (less than 3.2 defects per million scans).

Qwest VSS connects and interoperates with Agency networking environments as required in the RFP, including demilitarized zones (DMZs) and secure Local Area Networks as well as Internet connectivity. Authorized Agency representatives have access for on-demand VSS control [redacted]

6.4.1.2 Benefits of Vulnerability Scanning Services Technical Approach (L.34.1.6.1(b))

Qwest's VSS provides a manageable, scalable, and repeatable process that provides the validity and assurance that comes with third-party assessments, without the need for additional Agency personnel resources or infrastructure to be deployed and managed. [redacted]

Figure 6.4.1-2. Features and Benefits of Qwest's Technical Approach

Feature	Benefit	[redacted]
On-Demand Service Architecture	Allows for centralized reporting, remediation workflow, and user management, while allowing scans to be distributed throughout an organization.	[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

Feature	Benefit	[redacted]
Continuously updated Vulnerability KnowledgeBase	As new signatures or product upgrades are deployed, Agencies immediately benefit from the new functionality. Agencies do not need to manage the upgrade process and always use the newest code ensuring that tests are performed with the latest known vulnerability checks.	[redacted]
Scanner Appliances Provided to Scan Internal Networks	Vulnerability scanning can be delivered to private networks by deploying the VSS SED. It requires no maintenance by the Agency and is installed in minutes. The SED requires no specific firewall configurations to obtain vulnerability updates.	[redacted]
Data communications are secured and stored data is encrypted	Complete end-to-end data protection is provided, enabling the Agency to trust the Qwest Team with their VSS requirements.	[redacted]
Browser-Based User Interface for Anytime Anywhere Access	Authorized Agency contact has on-demand access to VSS service at anytime from anywhere with browser-based access over the Internet.	[redacted]

Federal Enterprise Architecture (FEA) is an e-government initiative intended to serve as “a business-based framework for Government-wide improvement.” Qwest VSS advances the objectives of the FEA, as shown in ***Figure 6.4.1-3***.

Data contained on this page is subject to the restrictions on the title page of this proposal.

Figure 6.4.1-3. Qwest's VSS Advances FEA Requirements

FEA Requirement	
Enhance Cost Savings and Cost Avoidance	[redacted]
Improve Service Delivery	
Enhance Cost Savings and Cost Avoidance	
Increase Cross-Agency And Inter-Government Collaboration	
Improve Utilization of Government Information Resources	
Improve Performance Metrics	

6.4.1.3 Solutions to Vulnerability Scanning Service Problems (L.34.1.6.1(c))

The Qwest Team has learned from experience how to anticipate and solve problems that may arise over the course of service life. The problems described below are real; therefore, Qwest VSS has been designed to be

Data contained on this page is subject to the restrictions on the title page of this proposal.

non-intrusive and signatures are designed not to adversely impact the scanned devices, as shown in ***Figure 6.4.1-4***.

Figure 6.4.1-4. Potential VSS Problems and Qwest Solutions

Problem	[redacted]
System crashes when scanned	[redacted]
Lack of Process to Get Systems Back Up and Running When a Crash Occurs	[redacted]
Updates not quickly deployed	[redacted]

The Qwest Team has put in place a process to fix any problem very quickly that may arise from our scanning activities. Also, when a fix is identified and approved by the Agency, it is immediately deployed. This process includes actively monitoring both the number of scans and the number of defects that result from scans. When comparing the number of device scans to the number of issues, the results are compelling. [redacted]

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

6.4.2 Satisfaction of Vulnerability Scanning Services Performance Requirements (L.34.1.6.2)

6.4.2.1 Vulnerability Scanning Services Quality of Service (L.34.1.6.2(a))

Qwest's VSS offering is designed to enable sustainable results at an operational level through a performance measurement system. This performance measurement system is based on the use of key performance metrics that meet GSA's AQLs. Active monitoring ensures that the Agencies are provided with the data they need to ensure that high performance is achieved [redacted] Qwest's VSS offering is fully compliant with the GSA requirements in ***Figure 6.4.2-1***.

Figure 6.4.2-1. Qwest's VSS Key Performance Metrics and AQLs

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	[redacted]
Availability	Routine	99.5%	≧ 99.5%	[redacted]
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	[redacted]
	With Dispatch	8 hours	≤ 8 hours	[redacted]

Availability: [redacted] Qwest will collaborate with

Data contained on this page is subject to the restrictions on the title page of this proposal.

Agencies to define optimal appliance configurations to meet availability requirements for private scan deployments. [redacted]

Time to Restore: All troubles are recorded simultaneously via the [redacted] All troubles are recorded as "normal" or "urgent" [redacted] to the SOC for immediate attention. On a 24x7x365 basis, Qwest will detect, prioritize, isolate, diagnose, and repair faults affecting contract services and restore them to meet the Agency's specifications.

6.4.2.2 Approach for Monitoring and Measuring Vulnerability Scanning Services (L.34.1.6.2(b))

Qwest's approach is to continually monitor the availability and performance of the key components of the VSS, including the servers and systems in the SOC and perimeter and scanner appliances in the Agency environment, using the VSS performance monitoring system. This system provides the Qwest Team with graphical representations of numerous system parameters, tracks configuration changes, and collects error messages. It also provides exception-based alerting if certain values reach defined thresholds.

[redacted]. All systems in the VSS platform are monitored [redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]. A failure to respond to the probe triggers a notification to the SOC, and corrective action is taken.

[redacted]New tools that may also provide enhancements are continually investigated. The VSS solution will notify the Agency Point of Contact (POC) and Qwest SOC if a scan or map fails to launch because an appliance is offline. The Qwest SOC will follow up with the POC to further troubleshoot the issue.

6.4.2.3 Verification of Vulnerability Scanning Services (L.34.1.6.2(c))

Qwest's VSS AQL compliance is verified through a combination of internal audit, test, and verification processes, trouble ticket records, and executive summary reports. [redacted] The network will be probed periodically to collect VSS availability data. Determining availability based upon alarms (and associated trouble tickets) is the least intrusive and normal approach used. At the end of each evaluation period, as established in the VSS AQL, availability and TTR will be calculated. [redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

6.4.2.4 Vulnerability Scanning Services Performance Improvements (L.34.1.6.2(d))

[redacted]

6.4.2.5 Additional Vulnerability Scanning Service Performance Metrics (L.34.1.6.2(e))

[redacted]

6.4.3 Satisfaction of Vulnerability Scanning Service Specifications (L.34.1.6.3)

The following sections describe how Qwest will satisfy the specifications of VSS.

6.4.3.1 Satisfaction of Vulnerability Scanning Service Requirements (L.34.1.6.3(a))

Qwest fully complies with all mandatory stipulated and narrative capabilities, features, and interface requirements for VSS. The following ***Figure 6.4.3-1*** and Sections 6.4.3.1.2 and 6.4.3.1.3 summarize Qwest's response to the VSS capabilities listed in RFP C.2.10.3.1.4, features of RFP C.2.10.3.2, and interfaces of RFP C.2.10.3.3. These subsections are

Data contained on this page is subject to the restrictions on the title page of this proposal.

intended to provide the technical description required per L.34.1.6.3(a) and do not limit or caveat Qwest's compliance in any way.

6.4.3.1.1 Satisfaction of VSS Capability Requirements (L.34.1.6.3(a); C.2.10.3.1.4)

Figure 6.4.3-1 provides a comprehensive list of Qwest's VSS capabilities with respect to GSA's service requirements.

Figure 6.4.3-1. Qwest's VSS Meets GSA's Capabilities Requirements

Required VSS Capabilities	[redacted]
1. The contractor shall support the Agency in establishing, implementing, and maintaining a vulnerability scanning service, which shall be operational on a 24x7x365 basis. The service shall provide the following:	[redacted]
a. External Vulnerability Scanning, which tests Internet connected nodes in the network, including Web environments.	[redacted]
b. Internal Vulnerability Scanning, which looks for local/host flaws and internal threats, usually inside the firewall.	[redacted]
2. The systems shall periodically probe networks, including operating systems and application software, for potential openings, security holes, and improper configuration.	[redacted]
3. The contractor shall probe Agency systems for vulnerabilities in, but not limited to, the following areas as applicable:	[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

Required VSS Capabilities	[redacted]
a. Back Doors	[redacted]
b. Bind	[redacted]
c. Browser	[redacted]
d. Brute Force Attacks	[redacted]
e. Common Gateway Interface-Binary (CGI-Bin)	[redacted]
f. Daemons	[redacted]
g. Distributed Component Object Model (DCOM)	[redacted]
h. Databases	[redacted]
i. Domain Name Service	[redacted]
j. eCommerce Applications	[redacted]
k. Email	[redacted]
l. Firewalls	[redacted]
m. File Sharing	[redacted]
n. File Transfer Protocol (FTP)	[redacted]
o. General Remote Services	[redacted]
p. Hardware and Network Appliances	[redacted]
q. Hubs	[redacted]
r. Information/Directory	[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

Required VSS Capabilities	[redacted]
Services	[redacted]
s. Instant Messaging	[redacted]
t. Lightweight Directory Access Protocol (LDAP)	[redacted]
u. Mail Applications	[redacted]
v. Multimedia Internet Mail Extension	[redacted]
w. Network	[redacted]
x. Network Sniffers	[redacted]
y. Netbios	[redacted]
z. Network File System (NFS)	[redacted]
aa. Network Information System (NIS)	[redacted]
bb. NT-Critical Issues	[redacted]
cc. NT-Groups	[redacted]
dd. NT-Networking	[redacted]
ee. NT-Password Checks	[redacted]
ff. NT Policy Issues	[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

Required VSS Capabilities	[redacted]
gg. NT Registry	[redacted]
hh. NT-Services	[redacted]
ii. NT-Users	[redacted]
jj. Port Scans	[redacted]
kk. Protocol Spoofing	[redacted]
ll. Router-Switch	[redacted]
mm. Remote Procedure Call (RPC)	[redacted]
nn. Shares	[redacted]
oo. Simple Mail Transfer Protocol	[redacted]
pp. Simple Network Management Protocol (SNMP)	[redacted]
qq. Server Message Block (SMB)	[redacted]
rr. Transmission Control Protocol/Internet Protocol (TCP/IP)	[redacted]
ss. Trojan Horses	[redacted]
tt. Web Scans	[redacted]
uu. Web Servers	[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

Required VSS Capabilities	[redacted]
vv. Wireless Access Points	[redacted]
ww. X-Windows	[redacted]
4. The contractor shall proactively identify network vulnerabilities and propose appropriate countermeasures, fixes, patches, and workarounds.	[redacted]
5. The contractor shall notify the Agency of vulnerabilities discovered via email, pager, fax, or telephone as directed by the Agency.	[redacted]
6. The contractor shall also provide the Agency with secure Web access to vulnerability information, scan summaries, device/host reports, and trend analyses.	[redacted]
7. The contractor shall review vulnerabilities discovered with the Agency, as required.	[redacted]
8. The contractor shall provide scan scheduling flexibility to the Agency in order to minimize any interruptions in normal business activities.	[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

Required VSS Capabilities	[redacted]
	[redacted]
9. The contractor shall provide the Agency with non-destructive and non-intrusive vulnerability scans that will not crash the systems being analyzed or disrupt Agency operations. The scans shall not provoke a debilitating denial of service condition on the Agency system being probed.	[redacted]
10. The contractor shall use other analytical means to ascertain the vulnerability of Agency systems if a particular scan is potentially destructive or intrusive.	[redacted]
11. The contractor shall ensure that the scanning engine is regularly updated with new vulnerabilities information in order to maintain effectiveness of the service.	[redacted]
12. The contractor shall support networks of varying size and complexity.	[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

6.4.3.1.2 Satisfaction of VSS Feature Requirements (L.34.1.4.2(a); C.2.10.3.2.1)

[redacted]

6.4.3.1.3 Satisfaction of VSS Interface Requirements (L.34.1.4.2(a); C.2.10.3.3)

Qwest provides all required interfaces based upon the capabilities of our proposed services as defined in IPS (RFP Section C.2.4.1), Premises-based IP Virtual Private Network Services (VPNS) (RFP Section C.2.7.2), and Network-based IP VPNS (RFP Section C.2.7.3).

6.4.3.2 Proposed Enhancements for Vulnerability Scanning Services (L.34.1.6.3(b))

[redacted]

6.4.3.3 Network Modifications Required for Vulnerability Scanning Service Delivery (L.34.1.6.3(c))

[redacted]

6.4.3.4 Experience with Vulnerability Scanning Service Delivery (L.34.1.6.3(d))

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

As an element of our layered defense strategy, our customers enjoy the opportunity to conduct effective and proactive assessments of critical networking environments, enabling the rapid correction of vulnerabilities before they are exploited. Through this system, our customers have an online vulnerability management solution that evaluates the security of networks remotely providing for 24x7x365 detection and protection by identifying real-world weaknesses.

6.4.3.5 Managed Tiered Security Services Approach (L.34.1.6.3(e))

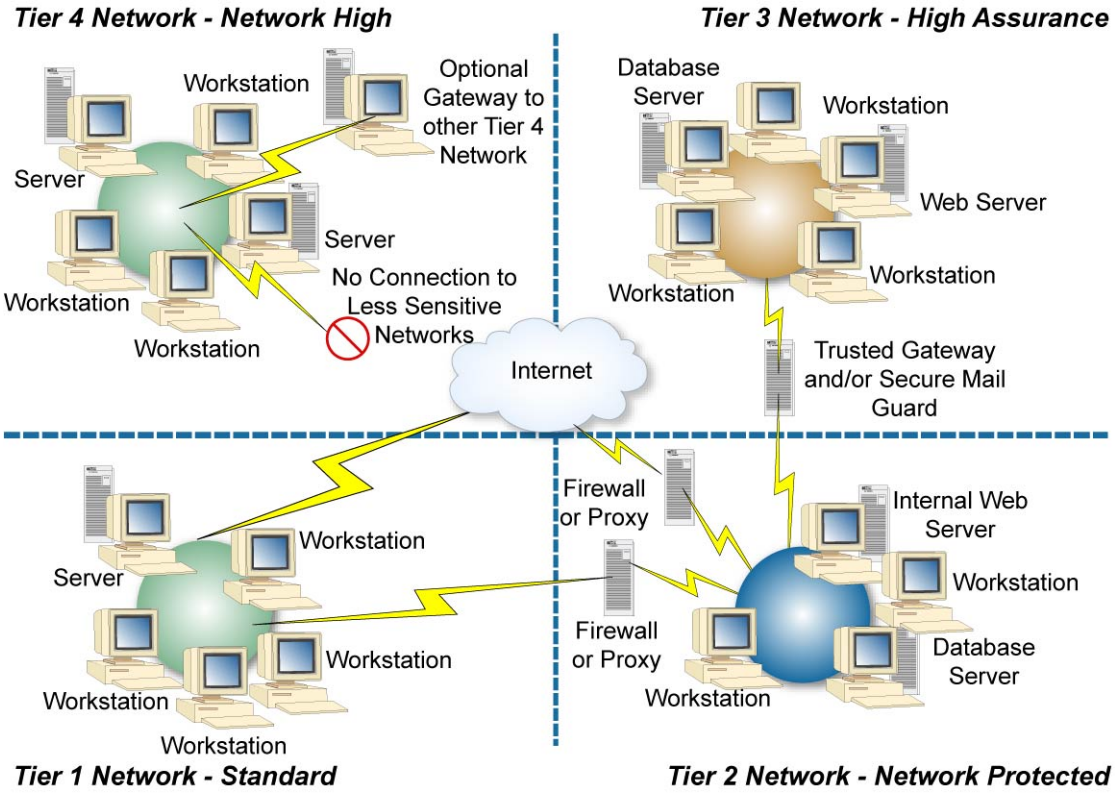
VSS is part of the Qwest MTSS technical solution. Design, implementation, and delivery according to GSA's Multi Tier Security Profiles (MTSP), ***Figure 6.4.3-3***, will be addressed to meet an Agency's requirements based on security service levels identified as described in Section 6.8.

MTSP Tier 2 – Protected Service shall provide security enhancements to the subscribing Agency with additional protection from unauthorized activities and the proliferation of malicious code. Protected service will also mitigate the potential for Denial of Service attacks. Security enhancements

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

Figure 6.4.3-3. MTSP Notional Architecture



193-2241

include a combination of firewall, premises-based VPN (encrypted tunnels), filtering router, proxy server, and boundary anti-virus detection technologies configurable to the subscribing Agency's security policy(s) and specifications.

Tier 2 is tailored to Sensitive but Unclassified mission functions and information. It employs both technical and network management components appropriate to the respective mission and/or information sensitivity.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.