6.2 OPTIONAL SECURITY SERVICES

This section presents Qwest's proposed optional services for the Networx program. In our selection of optional services we applied two criteria:

- Does the Qwest Team have a market leadership position in the delivery of the optional service?
- Does the Qwest Team currently deliver the optional service to Federal Government customers?

The optional services proposed qualify for one or both of these criteria and offer the Networx Enterprise program a depth of capability that will facilitate transition and service convergence.

6.2.1 VULNERABILITY SCANNING SERVICE (VSS) (L.34.1.6.4, M.2.1.3)

Through our VSS offering, the Qwest Team 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 has teamed [redacted] to provide Agencies with security services defined by the RFP. The Qwest Team's VSS is a proven and effective service that meets the requirements of the RFP. 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. [redacted]

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

Qwest Team 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 [redacted]
- 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 vulnerabilities that are exploitable from the inside of networks

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

6.2.1.1 Reserved (L.34.1.6.4 (a))

6.2.1.2 Reserved (L.34.1.6.4 (b))

6.2.1.3 Technical Service Requirements (L.34.1.6.4 (c))

The Qwest Team's technical approach for VSS is to incorporate an on-demand, service-based vulnerability management solution through a trusted third-party operating a Security Operations Center (SOC), as opposed to

acquiring, installing, supporting, and maintaining an in-house product-based solution. [redacted]

6.2.1.3.1 Satisfaction of VSS Capability Requirements (L.34.1.6.4 (c), C.2.10.3.1.4)

Figure 6.2.1-1 provides a comprehensive list of the Qwest Team's VSS capabilities with respect to GSA's service requirements. Qwest fully complies with all mandatory stipulated and narrative capabilities requirements for VSS. The text in Figure 6.2.1-1 provides the technical description required per L.34.1.6.4(c) and does not limit or caveat Qwest's compliance in any way.

Figure 6.2.1-1. Qwest Team 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	[redacted]

Required VSS Capabilities	[redacted]
potential openings, security holes, and improper configuration.	
3. The contractor shall probe Agency systems for vulnerabilities in, but not limited to, the following areas as applicable:	[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 Services	[redacted]
s. Instant Messaging	[redacted]
t. Lightweight Directory Access Protocol (LDAP)	[redacted]
u. Mail Applications	[redacted]

Required VSS Capabilities	[redacted]
	[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]
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]

Required VSS Capabilities	[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]
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]

Required VSS Capabilities	[redacted]
8. The contractor shall provide scan scheduling flexibility to the Agency in order to minimize any interruptions in normal business activities.	[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]

6.2.1.3.2 Satisfaction of VSS Feature Requirements (L.34.1.6.4 (c), C.2.10.3.2.1)

[redacted]

6.2.1.3.3 Satisfaction of VSS Interface Requirements (L.34.1.6.4 (c), 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), PBIP-VPNS (RFP Section C.2.7.2) and NBIP-VPNS (RFP Section C.2.7.3).

6.2.1.4 Achieving Quality of Service Goals (L.34.1.6.4 (d))

The Qwest Team'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 Acceptable Quality Levels (AQLs). Active monitoring ensures that the Agencies are provided with the data they need to ensure that high performance is achieved. [redacted] The Qwest Team's VSS offering is fully compliant with RFP requirements in ***Figure 6.2.1-2***.

Figure 6.2.1-2. The Qwest Team'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%	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Availability: [redacted] In addition, Qwest will collaborate with Agencies to define optimal appliance configurations to meet availability requirements for private scan deployments. [redacted]

Time to Restore (TTR): All troubles are recorded [redacted] All troubles are recorded as "normal" or "urgent" [redacted] 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.

6.2.1.5 Proposed Service Enhancements (L.34.1.6.4 (e))

[redacted]

6.2.1.6 Qwest Experience (L.34.1.6.4 (f))

[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.

6.2.1.7 Approach to Performance Verification (L.34.1.6.4 (g))

Qwest VSS AQL compliance is verified through a combination of internal audit, test, and verification processes, trouble ticket records, and executive summary reports. 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]

6.2.1.8 Service Impact to Network Architecture (L.34.1.6.4 (h))

The only data that traverses the production transport network is reporting and command information generated by the internal scanning device. Qwest expects no impact to our network architecture due to the transmission of this traffic. Management and control of the production impact of scanning is wholly within the control of the Agency because it determines when and what is scanned.

6.2.1.9 Approach to Satisfying NS/EP Requirements (L.34.1.6.4 (i))

As defined in RFP Section C.5.2.2.1, VSS is not a National Security and Emergency Preparedness (NS/EP) impacted service. Qwest's overall support of the NS/EP requirements can be found in Section 3.5.1, and our NS/EP plan can be found in Appendix 2 to the Technical Volume.

6.2.1.10 Approach to Assured Service in the National Capital Region (L.34.1.6.4 (j))

Qwest is currently a leading provider of network services in the National Capital Region (NCR) with robust network architecture to ensure service continuity in the event of significant facility failures. Qwest has, and will continue to engineer, critical services to meet the requirements of each Agency to eliminate single points of failure for their network services.

Qwest understands the Government's requirement to assure performance of network services in and around the NCR. To meet this important requirement for VSS, Qwest has established Point-of-Presence (POP) diversity as well as VSS scanning devices inside and outside of the NCR. [redacted] Section 3.5.2 provides additional detail regarding our NCR infrastructure.

Qwest has recently acquired OnFiber, a metro SONET and Ethernet provider with yet another diverse network in the NCR. This gives Qwest at least three regional fiber optic networks to use to ensure redundancy and survivability in the greater Washington D.C. area.

The Qwest Team has multiple SOCs that are geographically diverse, and no MTSS is dependent on assets located solely within the NCR region.

6.2.1.11 Approach to Meeting Section 508 Provisions (L.34.1.6.4 (k))

According to RFP Section C.6.4, *Section 508 Provisions Applicable to Technical Requirements*, Section 508 provisions are not applicable to VSS. Qwest has fully described our approach to satisfying Section 508 requirements for applicable, offered services in Section 3.5.4, *Approach for Meeting Section 508 Provisions*, of this Technical Volume.

6.2.1.12 Approach to Incorporating Technological Enhancements and Improvements (L.34.1.6.4 (l))

Qwest has a proven, mature process that enables us to envision, research, evaluate, engineer, deploy, and operate new or emerging services including VSS. Driven initially by the Chief Technology Office, Qwest

evaluates new products and technologies for incorporation into the Qwest network, in partnership with Qwest Product Management.

[redacted]

[redacted]

Qwest suppliers participate fully in this process. Qwest assures compliance with suppliers by evaluating, testing, and certifying all emerging technology. The vendors on the Qwest Team are committed to driving new technologies and products. New technology, provided by suppliers, is driven through and implemented via NTSC process in order to standardize all new products and technologies we will present to Agencies.