6.2 MANAGED INTRUSION DETECTION AND PREVENTION SERVICE (L.34.1.6)

Qwest Intrusion Detection and Prevention Service, alone or in conjunction with other managed security services, provides the Agency with an effective deterrent to malicious attacks and end-user compliance issues that may otherwise impact confidentiality, integrity, and availability of Agency networks and systems.

The Qwest Team's Intrusion Detection and Prevention Service (IDPS) is a proven, established service that meets Government requirements and provides an effective deterrent to malicious attacks that could otherwise cause serious damage. Qwest IDPS provides a comprehensive management service, delivering two levels of tiered service, a multitude of capabilities, and a robust offering of Service Enabling Devices (SEDs) to meet Agency requirements. The two tiers of service offered are as follows:

- Tier 1 - provides IDPS support for up to and including 100Mbps
- Tier 2 - provides IDPS support for more than 100Mbps and up to and including 1Gbps

IDPS is an integral component of the Qwest Team's Managed Tiered Security Service (MTSS) offering that operates out of the Secure Operation Centers (SOCs) as shown in [redacted] The SOCs provide vital security services to both domestic and non-domestic Agency locations and commercial enterprises.

[redacted]

Figure 6.2-1 shows the MTSS architecture with IDPS working in conjunction with other security services. An Agency may choose IDPS alone or in combination with other services.

Qwest's IDPS meets all the mandatory requirements from Sections C and J of the Request for Proposal (RFP). Qwest's IDPS capabilities include:

- A service based on the requisite security standards and network connectivity
- A proven, reliable agent system for collecting intrusion information from a wide variety of sensors
- Transmission of the encrypted information from Agency locations to the SOC in near real time
- Use of models based upon heuristics, policies, and profiles to determine attacks, severity, and appropriate courses of action
- Immediate, automatic response to attacks per established standard operating procedures with each Agency
- Clear, visible methods for verifying and reporting on performance metrics
- More than 1,000 highly skilled professional staff to provide lessons learned, resolve attacks or other problems, and provide IDPS design and implementation services for Agencies
- A record of successful services to a large number of Government Agencies and enterprise customers

6.2.1 Technical Approach to Intrusion Detection and Prevention Service Delivery (L.34.1.6.1)

The Qwest technical approach for IDPS is addressed in the following sections.

6.2.1.1 Approach to Intrusion Detection and Prevention Service Delivery (L.34.1.6.1(a)

Qwest's IDPS meets all requirements specified in the RFP. IDPS is available today to reduce or avoid service disruptions from malicious attacks. Qwest offers Agencies effective systems and processes to monitor their networks for attacks such as misuse, anomalies, detection, recording of intrusions and intrusion attempts, and performance of corrective response. Qwest’s IDPS meets the required functional capabilities, standards and connectivity.

IDPS Necessary Functions. The Qwest IDPS uses intrusion sensors to analyze packet activity on the Agency’s network, detect malicious activities, and report these to the SOC(s) via encrypted transport in near real-time. The SOC(s) use a robust Security Information Management (SIM) system complete with on-site, secure, fault-resilient data storage. This system enables the SOC(s) to correlate security events from multiple devices and data sources, improving the accuracy and confidence level of threat detection. An IDPS SED can be deployed in a number of configurations depending on the Agency’s needs. IDPS technology (when deployed inline and active) actively blocks potentially malicious traffic based on heuristics and signature files. IDPS can take automatic corrective action without requiring human intervention. The SOC will alert the Agency that traffic has been blocked and works with the Agency to either continue the block or allow the traffic to pass.

Target Criticality**.** If a critical application is under attack, the SOC will increase the priority of this event. Critical applications are identified and prioritized by the Agency and inserted into the SIM by the SOC. Examples of critical applications include sensitive databases or network attached supervisory control terminals.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Compliance with Required Standards. Qwest IDPS complies with all the U.S. security standards, as shown in ***Figure 6.2.1-1***. The system is continuously updated as new versions and signatures are introduced. These standards include Federal Information Security Management Act (FISMA), National Institute of Standards and Technology Federal Information Processing Standards Publication (NIST FIPS PUB) 140-2, NIST Special Pub 800-31, NIST PUB 199, and United States Computer Emergency Readiness Team (US-CERT).

Figure 6.2.1-1. Qwest's IDPS Meets All General Services Administration Required Standards

Qwest IDPS Meets All General Services Administration (GSA) Required Standards	
E-Government Act of 2002, Title III (FISMA)	NIST FIPS PUB 199 — Standards for Security Categorization of Federal Information and Information Systems
NIST FIPS PUB 140 - 2 — Security Requirements for Cryptographic Modules	US-CERT Reporting Requirements
NIST Special Publication 800-31 — Intrusion Detection Systems (IDS)	All Appropriate Standards for any Applicable Underlying Networx Access and Transport Services
All New Versions, Amendments, and Modifications of the Above when Offered Commercially.	NIST Special Publication 800-51, Use of the Common Vulnerabilities and Exposures Naming Scheme

IDPS Provides Required Connectivity. The Qwest IDPS interoperates with Agency networking environments, including demilitarized zones, secure Local Area Networks, and support of connectivity to extranets and the Internet.

6.2.1.2 Expected Benefits of Intrusion Detection and Prevention Service Technical Approach (L.34.1.6.1(b))

Qwest's IDPS provides several important benefits to Agencies, as summarized in ***Figure 6.2.1-2.***

Figure 6.2.1-2. Features and Benefits of Qwest IDPS

Feature	Benefit	Substantiation
Certified security staff	Qwest's relationship [redacted] provides strength, depth, and experience to our managed security services portfolio. The combination [redacted] intellectual capital in tandem with Qwest's extensive managed services business	The Qwest Team has more than 1,000 professionals in the security practices group serving commercial, Governmental, and wholesale clients. The Managed Security Service (MSS) staff includes board-certified protection professionals (CPP - American Society for Industrial Security International), and

Feature	Benefit	Substantiation
	provides the Agency with a trusted source in which to provide IDPS.	other security-related certifications.
Heuristic-based SOC management toolset	State-of-the-art, customized management and monitoring system enables fault resolution and aids in threat mitigation.	Qwest deploys SOC SIM agent at the Agency premises in order to actively manage and monitor IDPS alerts. This toolset provides the Agency with an IDPS service that identifies real alerts and bypasses most false positive alerts.
Customer-focused MSS practices discipline.	Qwest's approach to IDPS is based in application management and control. We provide a cost-effective service and manage it holistically with other network-based transport services.	[redacted]
Scaleable SOC infrastructure platform	Qwest's proven capability, combined with the steady application of lessons learned and alerts to thousands of organizations provides an Agency with an extensible SOC platform.	Qwest IDPS can support an Agency's desire to deploy gateway-based and/or host-based implementations supporting most existing IDS/IDPS hardware and software in which an Agency might have already invested [redacted]

Figure 6.2.1-3 shows how the Qwest IDPS addresses the objectives of the Federal Enterprise Architecture (FEA). The breadth and depth of our security practice and lessons learned support FEA objectives.

Figure 6.2.1-3. FEA Objectives. *Qwest IDPS supports FEA objectives for improved utilization of Government information resources, cost savings and avoidance, and increased collaboration.*

FEA Requirement	How Qwest supports FEA Objectives
Improve utilization of Government information resources	The Qwest Team leverages our experience and lessons learned to improve security techniques, such as threat signatures, better and faster than a single Agency. This allows Agencies to focus on core missions and service delivery to constituents.
Enhance cost savings and cost avoidance through a mature FEA Government-wide	Qwest IDPS identifies potential network threats and reduces network disruptions, thus achieving cost avoidance.
Increase cross-Agency and inter-Government collaboration	Qwest enables Agencies to practice safe inter-Agency communications with the knowledge that Qwest IDPS-protected Agencies will not harbor attacking hosts.

6.2.1.3 Solutions to Intrusion Detection and Prevention 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 IDPS lifecycle. [redacted] We codify the lessons learned and use them to make continuous process improvements in our methods. Two examples of IDPS problems and solutions appear in [redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Qwest will continuously improve our methods based on lessons learned. This is vital to Agency satisfaction.

6.2.2 Satisfaction of Intrusion Detection and Prevention Service Performance Requirements (L.34.1.6.2)

Qwest's IDPS meets all defined KPIs and AQLs.

6.2.2.1 Intrusion Detection and Prevention Service Quality of Services (L.34.1.6.2(a))

Qwest's IDPS performance metrics are summarized in ***Figure 6.2.1-5***.

Figure 6.2.1-5. Qwest IDPS Key Performance Indicators

KPI	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	[redacted]
Availability	Routine	99.5%	≥ 99.5%	[redacted]
Event Notification (EN)	Routine	Within 24 hours of a Low category event	≤ 24 hours	[redacted]
		Within 10 minutes of a High category event	≤ 10 minutes	[redacted]
Grade of Service (Configuration /Change)	Routine	Within 5 hours for a Normal priority change	≤ 5 hours	[redacted]
		Within 2 hours for an Urgent priority change	≤ 2 hours	[redacted]
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	[redacted]
	With Dispatch	8 hours	≤ 8 hours	[redacted]

Availability: Qwest IDPS is delivered through industry-leading security appliances [redacted] Our alert monitoring tools can isolate potential service disruptions prior to full network fault.

Event Notification (EN): Qwest's proactive network monitoring capabilities correlate network performance statistics and alerts, ultimately triggering performance thresholds that automatically create notification trouble tickets [redacted] Qwest's SOC will immediately notify the predetermined Agency contact and initiate triage on the alert or EN.

Grade of Service (Configuration/Change): Configuration Changes can be requested by the Agency [redacted]

Changes initiated by Qwest require Agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency). Qwest guarantees normal configuration changes within five hours and within two hours for urgent changes.

Time to Restore (TTR): All troubles are recorded simultaneously [redacted] 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.

6.2.2.2 Approach for Monitoring and Measuring Intrusion Detection and Prevention Services (L.34.1.6.2(b))

To ensure AQLs are met and that critical issues are immediately addressed, thresholds are set depending on the nature of the event. The events are tracked via individual tickets that are prioritized based on classification and response time AQLs. Performance levels and AQL of KPIs are monitored [redacted] The ticket is subsequently tracked and updated for technical and AQL performance throughout the escalation process until successful closure.

Qwest recognizes that it is the Government's intent that KPI monitoring of services is included in the scope of work to be performed. [redacted]

[redacted]

[redacted]

6.2.2.3 Verification of Intrusion Detection and Prevention Services (L.34.1.6.2(c))

The SOC will manage and report on KPIs for Agency IDPS configurations [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

6.2.2.4 Intrusion Detection and Prevention Services Performance Improvements (L.34.1.6.2(d))

[redacted]

6.2.2.5 Additional Intrusion Detection and Prevention Service Performance Metrics (L.34.1.6.2(e))

[redacted]

6.2.3 Satisfaction of Intrusion Detection and Prevention Service Specifications (L.34.1.6.3(a))

Qwest fully complies with all mandatory stipulated and narrative capabilities, features, and interface requirements for IDPS. Figure 6.2.3-1 and Section 6.2.3.1.2 summarize Qwest's response to the Managed Firewall Service (MFS) capabilities listed in RFP C.2.10.2.1.4, features of RFP C.2.10.2.2, and interfaces of RFP C.2.10.2.3. These subsections are 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. Below we discuss how these are satisfied, summarize our experience, and reference our MTSS proposal section covered in detail in Section 6.8.

6.2.3.1 Satisfaction of Intrusion Detection and Prevention Service Requirements (L.34.1.6.3(a))

6.2.3.1.1 Satisfaction of IDPS Capability Requirements (L.34.1.4.2(a); C.2.10.2.1)

The IDPS technical capabilities shown [redacted] are essential to achieve an effective service and high degree of customer satisfaction. We comply with all 31 requirements and work closely with Agencies to design, implement, and operate the IDPS in accordance with them.

Figure 6.2.3-1. Qwest provides required IDPS capabilities

Required IDPS Capabilities	[redacted]
1. Qwest will provide design and implementation services. This will enable the Agency and the contractor to discuss matters such as system recommendations, a baseline assessment, rules, signature sets, configurations, and escalation procedures.	[redacted]
2. Qwest will provide installation support to include testing of equipment, testing of software, and loading of any Agency relevant data, as required by the Agency.	[redacted]
3. Qwest will provide intrusion detection software and hardware components to include sensors, taps, and switches, as applicable.	[redacted]

Required IDPS Capabilities	[redacted]
4. Qwest will provide host intrusion detection in order to protect critical Agency servers. The contractor shall monitor the servers for security breaches and misuse while enforcing best industry practices and Agency security policies.	[redacted]
5. Qwest will perform a scan of the intrusion detection system to verify the integrity of service components and validate installation and configuration activities.	[redacted]
6. Qwest will support remote monitoring capabilities and proactively monitor the network on a 24x7x365 basis for indications of compromise, such as intrusions, anomalies, malicious activities, and network misuse.	[redacted]
7. Qwest will detect precursor activities, such as unauthorized network probes, sweeps, and scans that may indicate a potential attack.	[redacted]
8. Qwest will perform anomaly detection in order to identify typical traffic trends and unusual behaviors that may indicate a potential attack.	[redacted]

Required IDPS Capabilities	[redacted]
9. Qwest will perform signature-based detection and analyze system activity for known attacks such as, but not limited to: a. Buffer Overflows b. Brute Force c. Denial of Service d. Reconnaissance Efforts	[redacted]
10. Qwest will monitor the network for signatures that take advantage of vulnerabilities identified in the SANS/FBI (SysAdmin, Audit, Network, Security Institute/Federal Bureau of Investigation) Twenty Most Critical Internet Security Vulnerabilities list.	[redacted]
11. Qwest will automatically update the signature sets in use as new signatures become available.	[redacted]
12. Qwest will support Agency-defined signatures in the signature database for increased security as required by the Agency.	[redacted]
13. Qwest will perform policy-based detection to reveal violation of Agency security policies and detect potentially harmful traffic not intercepted by the firewall.	[redacted]
14. Qwest will provide alerts based on known vulnerabilities and Agency security policies.	[redacted]
15. Qwest will analyze suspicious security alerts to determine the significance of an event and immediately notify the Agency when the event is deemed of high priority. This focuses attention on real threats without greatly affecting legitimate traffic and minimizes false alarms.	[redacted]
16. Qwest will notify the Agency of events via email, pager, fax, or telephone, as directed by the Agency.	[redacted]

<table>
<tr><th>Required IDPS Capabilities</th><th>[redacted]</th></tr>
<tr><td>17. Qwest will provide the Agency with immediate access to severe alert information, which shall contain but not be limited to the following:
a. Incident Description
b. Incident Target
c. Incident Origin
d. Potential Incident Impacts
e. Incident Remedies
f. Incident Prevention Measures</td><td>[redacted]
[redacted]
<table>
<tr><th>[redacted]</th><th>[redacted]</th><th>[redacted]</th><th colspan="2">[redacted]</th></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
<tr><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td></tr>
</table></td></tr>
<tr><td>18. Qwest will respond dynamically to threats and take proactive and corrective actions to secure the network. These measures shall include but not be limited to the following, as applicable:
a. Automatic Termination of Affected Connections
b. Blocking Traffic from the Originating Host
c. Disconnecting Ports
d. Fixing the Vulnerability
e. Focusing the Monitoring on Suspicious Areas
f. Forwarding, Limiting, or Discarding Malicious Traffic</td><td>[redacted]</td></tr>
</table>

Required IDPS Capabilities	[redacted]
g. Logging off Users h. Modifying Configurations	
19. Qwest will recommend appropriate responses to attacks.	[redacted]
20. Qwest will employ defense mechanisms to detect and accurately stop attacks. These mechanisms include, but are not limited to: pattern-matching; protocol/traffic anomaly review; and stateful, deep-packet, and multi-packet inspection.	[redacted]
21. Qwest will advise the Agency on controlling and eliminating identified vulnerabilities.	[redacted]
22. Qwest will provide post-alarm support to include analysis and interpretation of attack data.	[redacted]
23. Qwest will ensure that suspected attack information is sent via secure means to the contractor's operation center for evaluation.	[redacted]

Required IDPS Capabilities	[redacted]
24. Qwest will provide the Agency with secure Web access to logs and service information, which shall contain but not be limited to the following, as applicable: a. Attack Name, Description, Level, Impact Date, Time and Remedies b. Change Requests c. Configuration Modifications d. Device Identification e. Intrusion Statistics f. Originating and Terminating IP Addresses g. Outages h. Originating and Terminating Port i. Protocol Affected j. Sensor IP Address k. Targeted Weaknesses l. Tickets m. Top Events n. Top Originating and Terminating IP Addresses	[redacted] [redacted] [redacted]
25. Qwest will perform configuration changes as initiated and prioritized by the Agency.	[redacted]
26. Qwest will maintain the intrusion detection system and perform necessary hardware/software upgrades, updates, and replacements.	[redacted]
27. Qwest will test and deploy the latest patches and bug fixes as soon as they become available in order to ensure optimal performance of the service.	[redacted]
28. Qwest will maintain the latest configuration information for restoration purposes.	[redacted]
29. Qwest will perform periodic security scans that are capable of revealing vulnerabilities of the	[redacted]

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

	Required IDPS Capabilities	[redacted]
	intrusion detection system.	[redacted]
30.	Qwest will document the results of the scans and the solutions to the identified vulnerabilities.	[redacted]
31.	Qwest will support networks of varying complexity with respect to size, bandwidth, and speeds.	[redacted]

6.2.3.1.2 Satisfaction of IDPS Interface Requirements (L.34.1.4.2(a); C.2.10.2.3)

Qwest is also fully compliant with the following required interfaces: Internet Protocol Service (RFP Section C.2.4.1), Premises-Based IP VPN Services (RFP Section C.2.7.2), and Network-Based IP VPN Services (RFP Section C.2.7.3).

6.2.3.2 Proposed Enhancements for Intrusion Detection and Prevention Services (L.34.1.6.3(b))

To enhance an Agency's ability to recognize and respond to network security events, if multiple managed security services are ordered during the course of this contract, [redacted]

6.2.3.3 Network Modifications Required for Intrusion Detection and Prevention Services Delivery (L.34.1.6.3(c))

Qwest requires no network modifications to deploy IDPS to Agencies. Qwest will conduct operational reviews to identify any specific Agency network modifications need for IDPS deployment.

6.2.3.4 Experience with Intrusion Detection and Prevention Services Delivery (L.34.1.6.3(d))

Qwest's IDPS is an integral component of our Managed Security Service Provider (MSSP) offering and is unique in its capabilities, because our service offerings extend beyond those of a typical MSSP. Our approach is to provide a customer-focused premium service that is vendor and device independent. This allows Agencies to retain their infrastructure intact. This also facilitates future upgrades and technology refreshments, providing Agencies with significant long-term benefits. We become a trusted advisor to them. [redacted]

Our experience is multi-dimensional; MSSP operations are a small part of a large security organization that can support all of our security recommendations. [redacted]

[redacted]

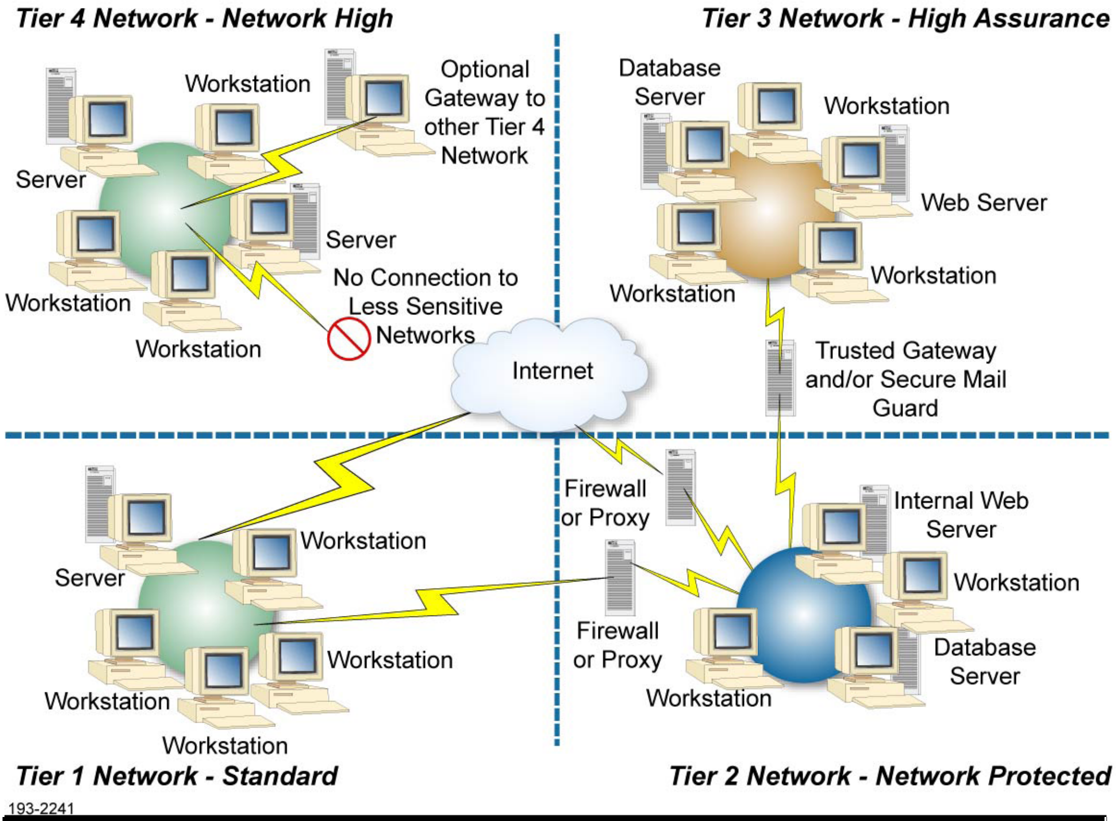
[redacted]

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

IDPS is part of the Qwest MTSS technical solution. Design, implementation, and delivery according to GSA's MTSP, as shown in ***Figure 6.2.3-2***, will be addressed to meet each Agency's requirements based on security service levels identified as described in Section 6.8. A defense in-depth strategy and technical solution that includes IDPS will be engineered as described in Section 6.8.3.1.1 to account for specific differences in each tier.

[redacted]

Figure 6.2.3-2. MTSP Notional Architecture



[redacted]

[redacted]