6.1.3 Intrusion Detection and Prevention Services (IDPS) (L.34.1.6, M.2.1.3)

The Qwest Team's IDPS, alone or in conjunction with other Managed Security Services (MSSs), 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.

Qwest has teamed [redacted] to provide Agencies with security services to fulfill the security baseline levels defined by the RFP. 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. The Qwest Team provides a comprehensive managed 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 100 Mbps
- Tier 2 - provides IDPS support for more than 100 Mbps and up to and including 1 Gbps

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. A variety of applications run within the SOC. Examples of these applications include the Security Information Manager (SIM), trouble ticketing system, control consoles, and reference databases.

[redacted]

Figure 6.1.3-1 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.

Our IDPS meets all the mandatory requirements from Sections C and J of the RFP. 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's 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 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
- Compliance with Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) security requirements

6.1.3.1 Technical Approach to Security Services Delivery (L.34.1.6.1, M.2.1.3 (b))

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

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

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

IDPS Necessary Functions. The Qwest Team's IDPS uses intrusion sensors to analyze packet activity on the Agency's network, detect malicious activities, and report these to the SOCs via encrypted transport in near real time. The SOCs use a robust SIM system complete with on-site, secure, fault resilient data storage. This system enables the SOCs 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 alerts 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 [redacted] 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. The Qwest Team's IDPS complies with all the U.S. security standards, as shown in ***Figure 6.1.3-2***. The system is continuously updated as new versions and signatures are introduced. These standards include FISMA, NIST Federal Information Processing Standards (FIPS) Publication 140-2, NIST Special Pub 800-31, NIST PUB 199, and US-CERT.

Figure 6.1.3-2. The Qwest Team's IDPS Meets All GSA Required Standards

Qwest Team IDPS Meets All General Services Administration 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	United States Computer Emergency Readiness Team (US-CERT) Reporting Requirements
NIST Special Publication (SP) 800-31 — Intrusion Detection Services (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 (SP) 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Naming Scheme

IDPS Provides Required Connectivity. The Qwest Team's IDPS interoperates with Agency networking environments, including de-militarized zones, secure Local Area Networks, and support of connectivity to extranets and the Internet.

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

The Qwest Team IDPS provides several important benefits to Agencies, as summarized in ***Figure 6.1.3-3.***

Figure 6.1.3-3. Features and Benefits of Qwest Team IDPS

Feature	[redacted]	[redacted]
Certified security staff	[redacted]	[redacted]
Heuristic-based SOC management toolset	[redacted]	[redacted]
Customer-focused Managed Tiered Security Services (MTSS) practices discipline.	[redacted]	[redacted]
Scaleable SOC infrastructure platform	[redacted]	[redacted]

Figure 6.1.3-4 shows how the Qwest Team's 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 6.1.3-4. FEA Objectives. *The Qwest Team IDPS supports FEA objectives for improved utilization of Government information resources, cost savings and avoidance, and increased collaboration.*

FEA Requirement	[redacted]
Improve utilization of Government information resources	[redacted]
Enhance cost savings and cost avoidance through a mature FEA Government-wide	[redacted]
Increase cross-Agency and inter-Government collaboration	[redacted]

6.1.3.1.3 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 codified the lessons learned and use them to make continuous process improvements in our methods. [redacted]

Figure 6.1.3-5. Anticipated IDPS Problems and Qwest Solutions

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

Of course, other problems may arise as well. We will continuously improve our methods based on the lessons learned. This is vital to Agency satisfaction.

6.1.3.2 Satisfaction of Security Services Performance Requirements (L.34.1.6.2, M.2.1.3 (c))

The Qwest Team's IDPS meets all defined Key Performance Indicators (KPIs) and Acceptable Quality Levels (AQLs).

6.1.3.2.1 Quality of Services (L.34.1.6.2 (a))

The Qwest Team's IDPS performance metrics are summarized in ***Figure 6.1.3-6***.

Figure 6.1.3-6. The Qwest Team's IDPS Key Performance Indicators (KPIs)

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: The Qwest Team's 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): The Qwest Team's proactive network monitoring capabilities correlate network performance statistics and alerts, ultimately triggering performance thresholds that automatically create notification trouble tickets [redacted] the Qwest Team'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 an Agency [redacted]. Changes initiated by us require Agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency). We guarantee normal configuration changes within five hours and within two hours for urgent changes.

Time to Restore (TTR): All trouble issues are recorded [redacted] On a 24x7x365 basis, the Qwest Team will detect, prioritize, isolate, diagnose, and repair faults affecting contract services and restore them to meet the Agency's specifications.

6.1.3.2.2 Approach for Monitoring and Measuring KPIs and AQLs (C.2.10.2.4.1) (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. [redacted]

[redacted]

[redacted] The ticket is subsequently tracked and updated for technical and AQL performance throughout the escalation process until successful closure.

[redacted]

[redacted]

6.1.3.2.3 Verification of Intrusion Services (L.34.1.6.2 (c))

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

[redacted]

6.1.3.2.4 Proposed Performance Improvements (L.34.1.6.2 (d))

[redacted]

[redacted]

6.1.3.2.5 Additional Performance Metrics (L.34.1.6.2 (e))

[redacted]

6.1.3.3 Satisfaction of Security Services Specifications (L.34.1.6.3, M.2.1.3 (d))

The Qwest Team's IDPS satisfies each of the mandatory service requirements, including the required capabilities, features, and interfaces. The following sections discuss how these requirements are satisfied, address the required network modifications, summarize our experience, and reference our MTSS proposal section covered in detail in Section 6.11.

6.1.3.3.1 Satisfaction of Service Requirements (L.34.1.6.3 (a))

The Qwest Team will select technical solutions that best fit the Agency architecture, security and privacy profile requirements. Prior to implementing an IDPS solution, our technical personnel will conduct a design and implementation interview [redacted] with the Agency network administrator or appointed technical contact. Through this interchange meeting, we will discover the Agency's specific needs and required functionality and use this information to engineer the IDPS solution to meet Agency expectations.

6.1.3.3.1.1 Satisfaction of IDPS Capability Requirements (L.34.1.6.3 (a), C.2.10.2.1.4)

The IDPS technical capabilities shown in ***Figure 6.1.3-7*** are essential to achieve an effective service and high degree of Agency satisfaction. We comply with all 31 requirements and work closely with Agencies to design, implement, and operate the IDPS in accordance with them. Qwest fully complies with all mandatory stipulated and narrative capabilities requirements for IDPS. The text in Figure 6.1.3-7 provides the technical description required per L.34.1.6.3(a) and does not limit or caveat Qwest's compliance in any way.

Figure 6.1.3-7. The Qwest Team provides required IDPS capabilities

Required IDPS Capabilities	[redacted]
1. The Qwest Team will provide design and implementation services. This will enable an Agency and the contractor to discuss matters such as system recommendations, a baseline assessment, rules, signature sets, configurations, and escalation procedures.	[redacted]
2. We 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. The Qwest Team will provide intrusion detection software and hardware components to include sensors and taps and switches, as applicable.	[redacted]
4. The Qwest Team will provide host intrusion detection in order to protect critical Agency servers. We will monitor the servers for potential security breaches and misuse while enforcing best industry practices and Agency security policies.	[redacted]
5. The Qwest Team will perform a scan of the intrusion detection system to verify the integrity of service components and validate installation and configuration activities.	[redacted]
6. We 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]

Required IDPS Capabilities	[redacted]
7. The Qwest Team will detect precursor activities, such as unauthorized network probes, sweeps, and scans that may indicate a potential attack.	[redacted]
8. The Qwest Team will perform anomaly detection in order to identify typical traffic trends and unusual behaviors that may indicate a potential attack.	[redacted]
9. The Qwest Team 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 (DoS) d. Reconnaissance Efforts	[redacted]
10. The Qwest Team 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. The Qwest Team will automatically update the signature sets in use as new signatures become available.	[redacted]
12. The Qwest Team will support Agency-defined signatures in the signature database for increased security as required by the Agency.	[redacted]
13. The Qwest Team will perform policy-based detection to reveal violation of Agency security policies and detect potentially harmful traffic not intercepted by the firewall.	[redacted]
14. The Qwest Team will provide alerts based on known vulnerabilities and Agency security policies.	[redacted]

Required IDPS Capabilities	[redacted]
15. The Qwest Team 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. The Qwest Team will notify the Agency of events via email, pager, fax, or telephone, as directed by the Agency.	[redacted]
17. The Qwest Team 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	[redacted]
18. We 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 g. Logging off Users h. Modifying Configurations	[redacted]
19. We will recommend appropriate responses to attacks.	[redacted]

Required IDPS Capabilities	[redacted]
20. We 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. The Qwest Team will advise the Agency on controlling and eliminating identified vulnerabilities.	[redacted]
22. The Qwest Team will provide post-alarm support to include analysis and interpretation of attack data.	[redacted]
23. The Qwest Team will ensure that suspected attack information is sent via secure means to the contractor's operation center for evaluation.	[redacted]
24. The Qwest Team 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]

Required IDPS Capabilities	[redacted]
25. The Qwest Team will perform configuration changes as initiated and prioritized by the Agency.	[redacted]
26. The Qwest Team will maintain the intrusion detection system and perform necessary hardware/software upgrades, updates, and replacements.	[redacted]
27. We 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. The Qwest Team will maintain the latest configuration information for restoration purposes.	[redacted]
29. We will perform periodic security scans that are capable of revealing vulnerabilities of the intrusion detection system.	[redacted]
30. The Qwest Team will document the results of the scans and the solutions to the identified vulnerabilities.	[redacted]
31. The Qwest Team will support networks of varying complexity with respect to size, bandwidth, and speeds.	[redacted]

[redacted]

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

[redacted]

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

6.1.3.3.1.2 Satisfaction of IDPS Feature Requirements (L.34.1.6.3 (a), C.2.10.2.2)

There are no feature requirements listed under RFP Section C.2.10.2.2.

6.1.3.3.1.3 Satisfaction of IDPS Interface Requirements (L.34.1.6.3 (a), C.2.10.2.3)

The Qwest Team is also fully compliant with the following required interfaces: IPS (RFP Section C.2.4.1), PBIP-VPNS (RFP Section C.2.7.2), and NBIP-VPNS (RFP Section C.2.7.3).

6.1.3.3.2 Proposed Service Enhancements (L.34.1.6.3 (b))

[redacted]

[redacted]

[redacted]

6.1.3.3.3 Network Modifications (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.

6.1.3.3.4 Qwest Team Experience Delivering Intrusion Detection and Prevention Services (L.34.1.6.3 (d))

Qwest Team IDPS is an integral component of our Managed Security Service Provider (SSP) offering and is unique in its capabilities, because our service offerings extend beyond those of a typical SSP. Our approach is to provide an Agency-focused premium service that is vendor and device independent, allowing Agencies to retain their infrastructure intact. This also facilitates future upgrades and technology refreshments, providing our Agencies with significant long-term benefits; we become a trusted advisor. [redacted] Our experience is multi-dimensional. We have an experienced security organization that can support all of our security recommendations. [redacted]

[redacted]

[redacted]

[redacted]

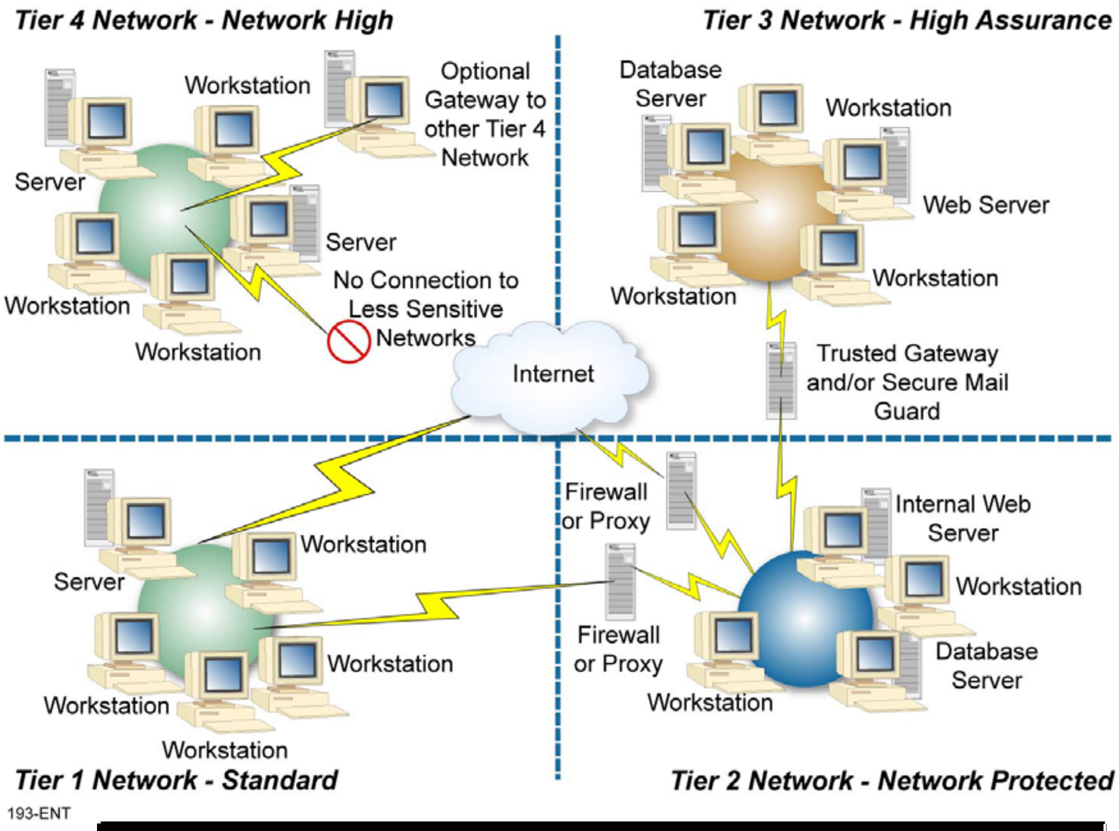
[redacted]

6.1.3.3.5 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 Section 6.0, as shown in ***Figure 6.1.3-10***, will be addressed to meet an Agency’s requirements based on security service levels. A defense in-depth strategy and technical solution that includes IDPS will be engineered to account for specific differences in each tier as described in Section 6.1.1 of the MTSP.

Figure 6.1.3-10. MTSP Notional Architecture



[redacted]

[redacted]