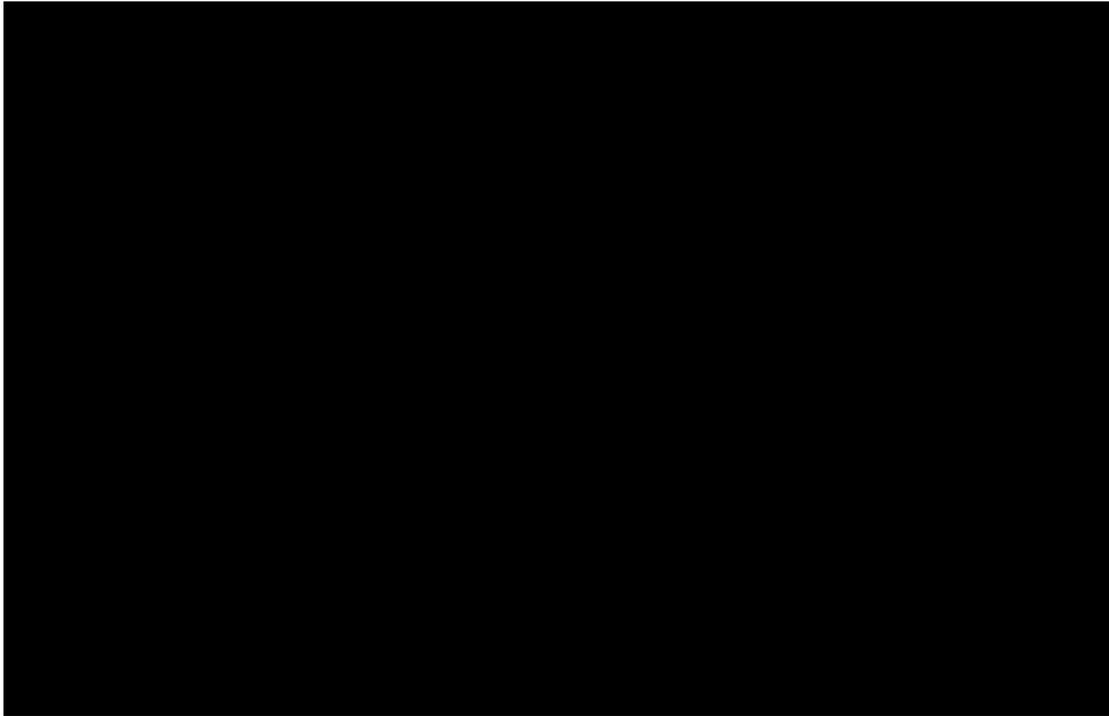


6.3 MANAGED E-AUTHENTICATION SERVICE (MEAS)

Qwest's MEAS offering provides a tightly integrated, cohesive service so that a variety of e-authentication mechanisms such as tokens, digital certificates, biometrics and other components appear to come from a single source.

Qwest's MEAS offering provides design, implementation, and operational capabilities for both token-based and certificate-based e-authentication services in a variety of hosting and operational environments. We also offer significant capabilities in identity management, access control and biometrics. Our service is provided by a unique and tightly integrated combination of services from Qwest, [REDACTED]. It is available globally, and supports connectivity via the Internet, Agency DMZs, and secure Local Area Networks (LANs). Qwest's MEAS capability offers optional services to meet additional Agency needs such as key management, roaming, and premium validation services. [REDACTED]

The Qwest Team provides the primary connectivity between users, servers, and the e-authentication services as well as the necessary user interfaces, including back-end services such as certificate authorities and registration authorities. These components are tightly integrated so that a user is presented with a cohesive service. Their organization and interrelation can be seen in **Figure 6.3-1**.



6.3.1 Technical Approach to Managed E-Authentication Service Delivery (L.34.1.6.1)

Qwest's MEAS is a fully-integrated enterprise solution designed to secure Intranet, extranet and Internet applications. MEAS enables fluid interaction with business partners, mobile workers, Web services, devices, and other users, all in compliance with the requirements. This highly-scalable service allows Agencies to rapidly establish a robust e-authentication system while alleviating the burden of certificate and token deployment, maintenance, and oversight. Agencies retain complete control over security policy, authentication models, and certificate and token management.

**6.3.1.1 Approach to Managed E-Authentication Service Delivery
(L.34.1.6.1(a))**

Qwest's MEAS consists of hardware and software components that provide for remote authentication of individual users over a network, for the purposes of electronic Government and commerce. Qwest's MEAS complies with the required standards.

Qwest's MEAS uses underlying transport and access services, permitting transfer of authentication information. It provides network connectivity to Agency demilitarized zones (DMZs), secure LANs, and public networks such as the Internet and organization extranets.

[REDACTED]

[Redacted]

[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

[Redacted]

Qwest MEAS allows Agencies to quickly, securely, and cost effectively issue digital certificates and tokens not only to employees, customers, and business partners, but also to Web services applications and network devices such as servers, routers and firewalls. Centralized, auditable root key generation, key escrow and distributed key recovery ensure maximum security and protection of private keys. The service also supports dual key-pair generation, allowing the separate issuance of encryption and signing key pairs.

Internationalization features include support for UTF-8 encoding, which allows enterprise users to enroll for and display digital IDs in languages that require non-ASCII characters [REDACTED]

[REDACTED] Easy-to-use toolkits and pre-integration with leading applications and platforms ensure rapid deployment of the e-authentication services on virtually any system, network, or device, whether located within the organization or externally. Qwest's MEAS has been proven under real-world conditions to scale smoothly from thousands to hundreds of thousands of users, allowing organizations to deploy digital certificates on an as-needed basis. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] We are committed to open standards, innovative technology, and strategic collaborations to promote the flexibility and ease of use Agencies need, not only to operate freely in diverse environments, but also to maximize return on existing investments.

[REDACTED]

[REDACTED] our next-generation MEAS platform allows Agencies to easily deploy digital identity management solutions to thousands of end users and enables seamless interoperability across heterogeneous systems and organization networks. [REDACTED]

[REDACTED]

[REDACTED] In addition, the solutions are particularly well suited to supporting secure access to organization networks through wireless LANs, VPNs, and other applications.

[REDACTED]

6.3.1.2 Benefits of Managed E-Authentication Services Technical Approach (L.34.1.6.1(b))

Qwest MEAS provides a flexible, scalable, and cost-effective means to enable e-authentication capabilities in a wide range of environments with unique requirements. The features, benefits, and substantiations of our service are presented in **Figure 6.3.1-2**, as follows.

Figure 6.3.1-2. Qwest MEAS Discriminators and Benefits

Feature	Benefit	
Qwest Team manages digital certificates and strong two- factor authentication tokens	Agencies can deploy authentication services on an outsourced basis.	[Redacted]
Government Standards compliant e- authentication, design, implementation, and operations	Agencies can leverage a range of e-authentication methods and tools appropriate to the specific level of security required.	[Redacted]
E-authentication Interoperability	Qwest's MEAS program is tightly integrated and offers a repeatable process so that the Agency can extend their e- authentication capabilities to other Agencies and suppliers.	[Redacted]

The benefits of our service in the context of the Federal Enterprise Architecture (FEA) are listed in **Figure 6.3.1-3**.

Figure 6.3.1-3. Qwest MEAS Meets FEA Requirements

Requirement	
Enhance Cost Savings and Cost Avoidance	[Redacted]
Increase Cross-Agency and Inter-Government Collaboration	[Redacted]
Improve Utilization of Government Information Resources	[Redacted]

6.3.1.3 Solutions to Managed E-Authentication Services Problems (L.34.1.6.1(c))

Successful delivery of MEAS is reliant on interoperability, network and system availability, and organizational security practices. We have addressed interoperability issues through a standards-based infrastructure. Network and

system availability is addressed through a redundant architecture. In **Figure 6.3.1-4** we present potential problems and our solution/mitigation approach.

Figure 6.3.1-4. Anticipated MEAS Problems and Qwest Solutions

Problem	
Unavailability of the platform.	[Redacted]
Many users are not e-authentication experts.	[Redacted]
Lost tokens or certificates create a security risk.	[Redacted]
Agencies may have unique networks, systems, architectures, and/or requirements.	[Redacted]

6.3.2 Satisfaction of Managed E-Authentication Services Performance Requirements (L.34.1.6.2)

6.3.2.1 Managed E-Authentication Services Quality of Service (L.34.1.6.2(a))

Qwest MEAS meet all performance requirements summarized in **Figure 6.3.2-1**. We have proven monitoring and measurement systems, procedures, and evaluation methods in place. The Government's required performance measures are in line with commercial measures and we are prepared to meet each of these performance requirements.

Figure 6.3.2-1. Qwest MEAS Key Performance Indicators (KPIs)

KPI	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	
Availability	Routine	99.99%	≥ 99.99%	[Redacted]
Event Notification (EN)	Routine	Within 4 hours of a Low category event (Severity 2 or 3)	≤ 4 hours	[Redacted]
		Within 30 minutes of a High category event (Severity 1)	≤ 30 minutes	[Redacted]
Grade of Service (GoS) (Configuration Change)	Routine	Within 24 hours for a Normal priority change (Severity 2 or 3)	≤ 24 hours	[Redacted]
		Within 2 hours for an Urgent priority change (Severity 1)	≤ 2 hours	[Redacted]

KPI	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	
Time To Restore (TTR)	Without Dispatch	4 hours (Severity 1)	≤ 4 hours	
	With Dispatch	8 hours (Severity 1)	≤ 8 hours	

Availability: Qwest MEAS is delivered through industry-leading technology platforms. Servers and systems that provide Qwest MEAS are designed for redundancy and scalability on carrier-class hardware. The architecture includes fully redundant data centers in different geographic locations with clustered servers, redundant power, and synchronized databases [REDACTED]

[REDACTED] There is no single point of failure that will disrupt operation.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

EN: Qwest’s proactive network monitoring capabilities correlates network performance statistics and triggers performance thresholds, which automatically create notification trouble tickets in NTM Remedy Trouble Ticket System. Thresholds levels are established to correspond with low (≤ 4 hours) and high category (≤ 30 minutes) events, which are subsequently communicated to the Agency.

GoS (Configuration/ Change): Configuration Changes can be requested by the Agency via the Qwest Control Networx Portal. Changes initiated by Qwest require Agency consent prior to implementation. Changes are categorized as Normal and Urgent (Emergency). Qwest guarantees normal configuration changes within 24 hours and within 2 hours for urgent changes. The Agency administrator can make certain GoS changes directly through the portal. Those changes go into effect in near real-time and enable the Agency to have independent control of their MEAS platform.

TTR: All troubles are recorded simultaneously via the [REDACTED] [REDACTED] Trouble Ticket System. All troubles are recorded as “normal” or “urgent” and routed [REDACTED] [REDACTED] to the Security Operations Center (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. Qwest will respond within 4 hours for troubles that do not require dispatch and will respond within 8 hours for troubles that require dispatch.

6.3.2.2 Approach for Monitoring and Measuring Managed E-Authentication Services (L.34.1.6.2(b))

Qwest’s approach is to continually monitor the availability and performance of the key components of the MEAS portfolio. Vital elements of MEAS are monitored for availability and performance by using our multi-dimensional performance monitoring system. This sophisticated, [REDACTED] [REDACTED] 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 Agency-defined thresholds.

[REDACTED]

6.3.2.3 Verification of Managed E-Authentication Services (L.34.1.6.2(c))

Qwest MEAS AQL compliance is verified through a combination of internal audit, test, and verification processes, trouble ticket records, and executive summary reports. An executive dashboard report provides an interactive summary of the overall MEAS performance. The report is complete with graphs, performance statistics, threat levels, help desk summaries, and vulnerabilities by service level. 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 MEAS AQL, availability and TTR will be calculated and AQL performance reports will be available to Agencies [REDACTED]

[REDACTED]

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 are monitored

[REDACTED]
[REDACTED] in order to ensure monitoring accuracy and to maintain a profile of Agency information security posture. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] The ticket is subsequently tracked and updated for technical and AQL performance throughout the escalation process until successful closure. Verification of MEAS requires extensive interaction and proactive monitoring capabilities combined with the expert knowledge of our SOC-certified security professionals. Our ability to identify events, triage, and respond meets the Agency's AQL requirements.

Qwest will provide all necessary monitoring as part of the service. The SOC lead engineer assigned to the Agency is responsible for monitoring and oversight of the performance of the Service Level Agreement after the service has been implemented. Qwest's delivery experience, combined with our knowledge that each Agency will have unique requirements, especially around GoS, allows the definition of appropriate change control processes and commitment levels by task order AQLs.

6.3.2.4 Managed E-Authentication Services Performance Improvements (L.34.1.6.2(d))

[REDACTED]
[REDACTED]

[REDACTED]

6.3.2.5 Additional Managed E-Authentication Services Performance Metrics (L.34.1.6.1(e))

[REDACTED]

6.3.3 Satisfaction of Managed E-Authentication Services Specifications (L.34.1.6.3)

The following sections describe how Qwest satisfies the specifications for MEAS.

6.3.3.1 Satisfaction of Managed E-Authentication Service Requirements (L.34.1.6.3(a))

Qwest MEAS offering is a fully-integrated solution designed to secure Intranet, extranet, and Internet applications while enabling fluid interaction with other Agencies, mobile workers, Web service devices, and other authorized users. This highly scalable service allows Agencies to rapidly establish a robust PKI and Certificate Authority (CA) system while avoiding the burden of PKI deployment, maintenance, and oversight. Agencies retain complete control over security policy, authentication models, and certificate life cycle management.

Built on open standards to ensure maximum flexibility, Qwest MEAS allows interoperability with virtually any application or device and is integrated with leading COTS, [REDACTED]

MEAS Design and Engineering Capabilities	[Redacted]
<p>The contractor shall support the Agency in developing detailed plans for implementation of user authentication service. The contractor shall offer to provide installation and integration support to the Agency, including but not limited to, testing of equipment and software, cost information, and loading of customer relevant data.</p>	[Redacted]

Figure 6.3.3-2. Qwest’s Token-Based Implementation Capabilities

MEAS Token-Based Implementation Capabilities	[Redacted]
<p>1. The contractor for the managed PKI service shall set up the authentication service at the identity authentication assurance level specified by the Agency and issue smart cards and/or other token devices in the quantities needed by an Agency, including.</p> <ul style="list-style-type: none"> a. Token Card, with or without Password, and Personal Identification Number (PIN) Pad b. Key Fob c. Soft Token 	[Redacted]
<p>2. The service shall follow the e-authentication federated authentication model to allow Agencies to validate multiple levels of authentication via a single interface, enable inter-Agency acceptance of digital certificates, and single sign-on capability.</p>	[Redacted]
<p>3. The contractor shall support the Agency-specified user ID naming scheme to meet Agency requirements.</p>	[Redacted]
<p>4. Implement SSL and/or TLS equipped servers as well as appropriate acceleration capabilities as required by the Agency to meet Agency performance requirements.</p>	[Redacted]

MEAS Token-Based Implementation Capabilities	
<p>5. Provide methods including, but not limited to, the following, as needed by the Agency:</p> <ul style="list-style-type: none"> a. PIN b. Authentication Methods based on Fingerprints. c. Network Authentication Systems and Servers for Embedded Devices (for example, routers, modem servers, and switches) 	[REDACTED]
<p>6 Contractor shall support in developing, implementing, and maintaining the AAA system and servers for network access, including the related tokens, based on but not limited to:</p> <ul style="list-style-type: none"> a. Remote Authentication Dial-In User Service (RADIUS) b. TACACS/TACACS+(Cisco) c. Diameter 	[REDACTED]

Figure 6.3.3-3. Qwest’s Token-Based Management Capabilities

MEAS Token-Based Management Capabilities	
<p>1. Manage and maintain the user authentication service including related tokens such as, but not limited to:</p> <ul style="list-style-type: none"> a. One-Time Passwords b. Smart Cards c. Hardware Tokens 	[REDACTED]
<p>2. Provide change management functions of the authentication service as requested by Agency designated points of contact (POCs) including, but not limited to:</p> <ul style="list-style-type: none"> a. Adding a New User b. Deleting a Current User c. Reset the PIN d. Changing, Adding, or Deleting IP Addresses of Software Agent e. User ID Administration 	[REDACTED]
<p>3. Ensure uninterrupted operations using mechanisms such as redundant servers that are located in geographically separate locations with the content continuously synchronized between them.</p>	[REDACTED]

Figure 6.3.3-4. Qwest MEAS Certificate-Based Implementation Capabilities

MEAS Certificate-Based Implementation Capabilities	
<p>1. Manage PKI that comprises, but is not limited to: CA, Registration Authority, Directory, and associated servers.</p>	<p>[REDACTED]</p>
<p>2. The contractor shall host and administer PKI certificates for an Agency including, but not limited to: certificate issuance, validation services, Agency application certificate registration, and management.</p>	<p>[REDACTED]</p>
<p>3. The contractor for the managed PKI service shall set up the authentication service at the identity authentication assurance level specified by the Agency and issue digital certificates in the quantities needed by an Agency.</p>	<p>[REDACTED]</p>
<p>4. The service shall follow the e-authentication federated authentication model to allow Agencies to validate multiple levels of authentication via a single interface, enable inter-Agency acceptance of digital certificates, and single sign-on capability.</p>	<p>[REDACTED]</p>
<p>5. The contractor shall establish a networking environment that provides the communication among PKI elements including, but not limited to, Certification Authorities (CA). The contractor shall implement SSL and/or TLS-equipped servers as well as appropriate acceleration capabilities as required by the Agency to meet Agency performance requirements.</p>	<p>[REDACTED]</p>

Figure 6.3.3-5. Qwest’s Certificate-Based Management Capabilities

MEAS Certificate-Based Management Capabilities	
1. The contractor for the managed PKI service shall maintain the database of: <ul style="list-style-type: none"> a. User Names b. User IDs c. Passwords 	
2. The contractor shall provide digital certificates and digital signatures within PKI as well as CA services.	
3. The contractor shall ensure uninterrupted operations using mechanisms such as redundant servers that are located in geographically separate locations with the content continuously synchronized among them.	
4. The contractor shall provide change management functions of the managed PKI service, as requested by Agency-designated POCs including, but not limited to: <ul style="list-style-type: none"> a. Adding a New User b. Deleting a Current User c. Resetting the Password d. Changing, Adding, or Deleting IP Addresses of Software Agent e. User ID Administration 	

6.3.3.1.2 Satisfaction of MEAS Features Requirements (L.34.1.4.2(a); C.2.10.6.2.1)

Qwest MEAS offering complies with the required features as enumerated in **Figure 6.3.3-6**.

Figure 6.3.3-6. Qwest’s MEAS Required Features

ID #	Name of Feature	Description	
1	Biometric Characteristics	The contractor shall provide biometric authentication methods including: iris scan, voice, and facial recognition, as required by the Agency.	[Redacted]
2	Encryption / Digital Signature Client Software	The contractor shall provide and support the encryption/digital signature client software for the Agency-designated POCs.	[Redacted]
3	E-Authentication Training	The contractor shall provide e-authentication training to Agency personnel as required. This includes, but is not limited to: user authentication, PKI, and CAs. The frequency and nature of training activities may vary according to Agency needs.	[Redacted]
4	Directory/Repository Function	The contractor shall develop, implement, and maintain a directory/repository function that will support the PKI and/or other e-authentication mechanism chosen by the Agency.	[Redacted]

6.3.3.1.3 Satisfaction of MEAS Interface Requirements (L.34.1.4.2(a); C.2.10.6.3)

Qwest provides all required interfaces based upon the capabilities of our proposed services as defined in: Frame Relay Service (Proposal Section 4.1.6), Asynchronous Transfer Mode Service (Proposal Section 4.1.7), Internet Protocol Service (Proposal Section 4.1.14), Premises-based IP VPN

[Redacted text block]

6.3.3.3 Network Modifications Required for Managed E-Authentication Services (L.34.1.6.3(c))

[Redacted text block]

6.3.3.4 Experience with Managed E-Authentication Services Delivery (L.34.1.6.3(d))

[Redacted text block]

[Redacted text] E-authentication services are delivered through our military-grade public key infrastructure and SOCs, ensuring

24x7x365 monitoring, management, and escalation across the globe. A sampling of our Government customers are described below

[Redacted content]

6.3.3.5 Managed Tiered Security Services (MTSS) Approach (L.34.1.6.3(e))

MEAS is part of the Qwest Networkx technical solution. Design, implementation, and delivery according to GSA's MTSP, as shown in **Figure 6.3.3-7**, will be addressed to meet an Agency's requirements based on security service levels identified as described in Section 6.8.

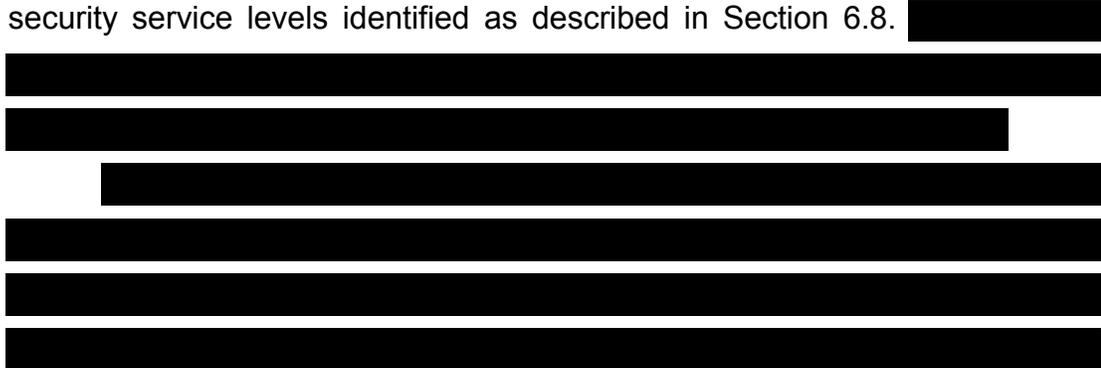
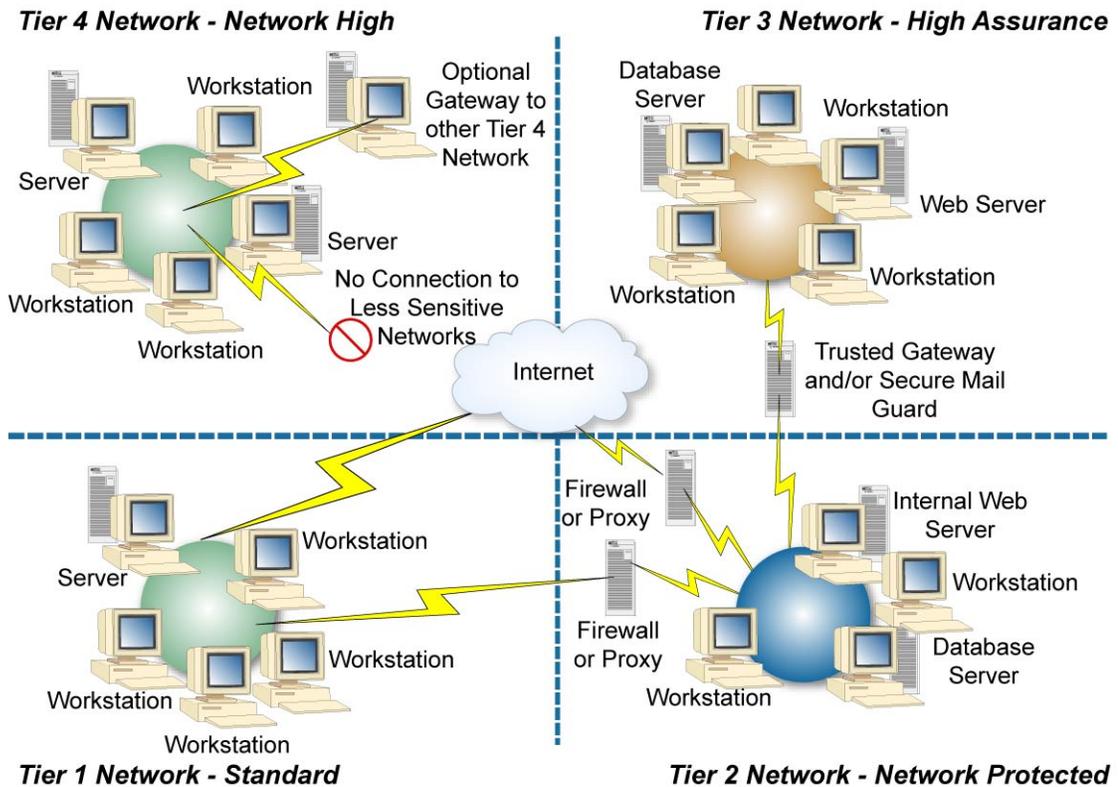


Figure 6.3.3-7. MTSP Notional Architecture



193-2241

[Redacted content]