

## **6.8 MANAGED TIERED SECURITY SERVICES (MTSS)**

### **(L.34.1.6)**

*Through our MTSS offering, Qwest provides Agencies with customized security solutions according to mission criticality and information sensitivity.*

Qwest has [REDACTED] to provide Agencies with security services to fulfill the security baseline levels defined by the Government. Specifically, security solutions will be customized for the Agency based on the respective level of mission criticality and information sensitivity. Each tiered service offering defines a level of protection for confidentiality, integrity and availability commensurate with the level of risk to Agency information and information assets. The Qwest Team complies with the tiered requirements for MTSS as defined in RFP Section C.2.7.4.1.4.1.

The Qwest Team will maintain security level performance standards and services that satisfy FISMA, while complying with individualized Agency requirements. The Qwest Team's comprehensive set of security services will meet all standards and interfaces required to maintain secure operations across Agency Intranets and interconnectivity from remote access users and collaboration partners for the operational life cycle of the system.

Based on the level of risk to the Agency asset base and the Federal Information Processing Standards (FIPS) 199 low-medium-high categorization for Agency information and information systems, Agencies will identify themselves with a security tier and will be provided corresponding security services. The delivered solution will be compliant with Agency security policy and the Agency's Federal Enterprise Architecture (FEA) security and privacy profile.

At a Tier 1 profile, the Agency implements all required security and the Qwest Team will provide help desk support for service delivery issues. In Tiers 2-4, the Qwest Team will provide the help desk and implement requested security services for each security level.

At a Tier 2 profile, the Qwest Team delivers services to protect the Agency from unauthorized and malicious activities associated with connectivity to other networks, including the Internet. The Qwest Team configures security devices such as firewalls, filter routers, proxy servers, and boundary anti-virus detection technologies to the requesting Agency's security policy and specification. Beyond the technical security enhancements, both physical and administrative protective features increase with the higher tiers and may vary in consonance with the mission criticality, information sensitivity, or unique user requirements. For example, Tier 3 and Tier 4 networks may draw requirements from National Information Assurance Certification and Accreditation Process (NIACAP) (NSTISSI 1000), Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP) (DoD 5200-40), and National Security Agency (NSA) Standards for handling of classified national security information (NSI) that exceed requirements for Federal Agencies detailed in Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) A-130, Appendix III. In developing the tailored implementations for Tier 3 and Tier 4 security profiles, communications, reliability, and network access will be critical factors. In the Tier 4 environment, all connectivity and data transfer will be between authorized Tier 4 peers in an isolated network environment that is air-gapped from all other tiers.

To support multi-level security requirements, security engineering and integration will emphasize technical solutions that enforce data separation

and network access. Access methods may include HyperText Transfer Protocol (HTTP), HyperText Transfer Protocol Secure (HTTPS), and File Transfer Protocol (FTP) for externally originated inquiries, or Web Push when a higher order Tier desires to provide access to a lower order Tier.

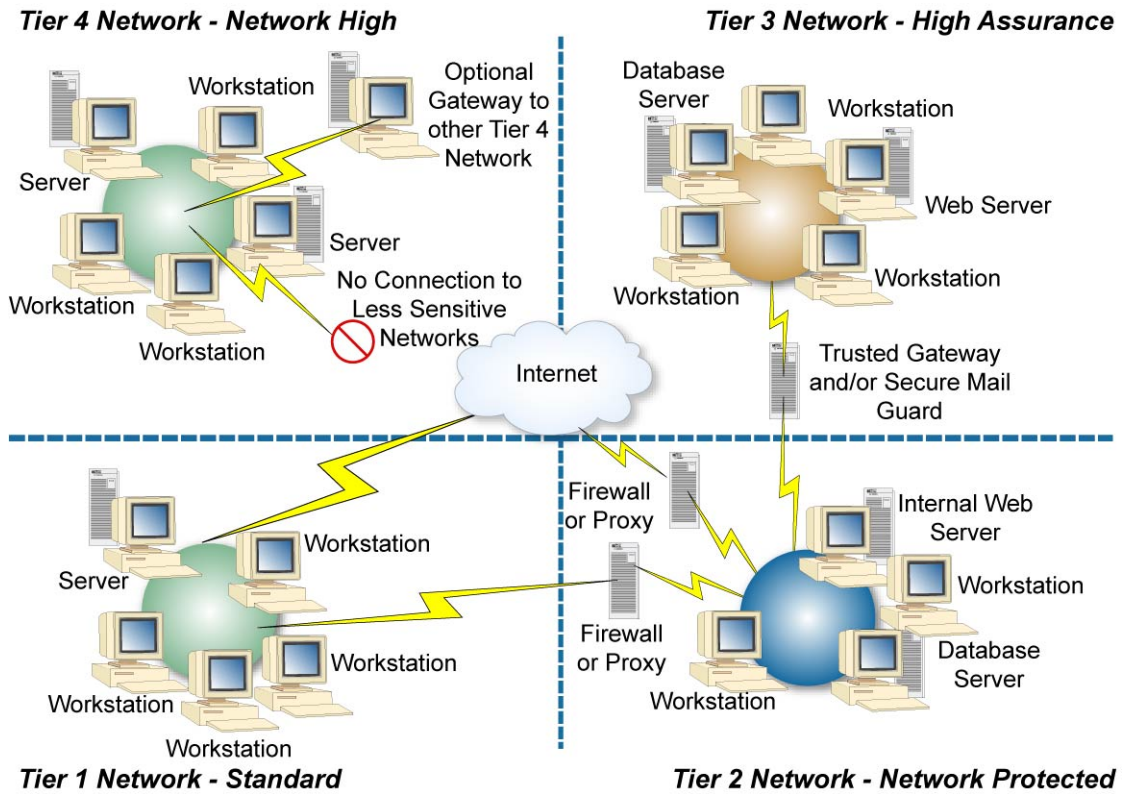
The Qwest Team will deliver security services commensurate with current and emerging threats. To ensure the continued viability of MTSS, the Qwest Team will review changes in technology and business practices, such as the use of Instant Messaging, peer-to-peer applications; develop open source intelligence to determine new internal and external threats from areas such as spyware, worms and vulnerability exploits, and coordinate with Agencies at the classified and unclassified level to maintain awareness of the technological and political threats that can impact their MTSS-provided service. Using this information, the Qwest Team will be able to use this analysis to adapt or recommend changes in technical, management, and operational controls to provide needed levels of protection for confidentiality, integrity, and availability—regardless of the tier profile.

### **6.8.1 Technical Approach to Managed Tiered Security Services Delivery (L.34.1.6.1)**

The goal of the GSA Multi-Tier Security Profiles (MTSP) initiative is to increase the security of data and telecommunications services delivered to Agencies. MTSS provides four baseline levels of security embedded in service delivery tier levels as shown in **Figure 6.8.1-1**.

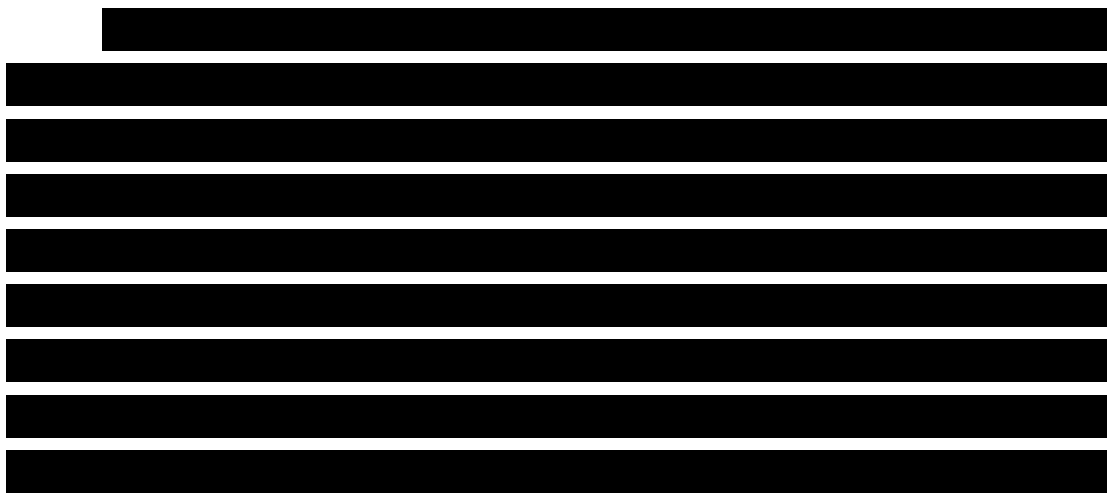
The Qwest Team will tailor the notional Tier 1 to Tier 4 architectures to individual Agency's requirements based on levels of mission criticality and information sensitivity and applicable compliance requirements defined in sources such as FISMA, DITSCAP, and NSI handling guidance. By looking at security as an integral part of the systems engineering solution, the Qwest

**Figure 6.8.1-1. MTSP Notional Architecture**



193-2241

Team's MTSP solution sets will provide the same level of performance as would be expected for the basic transport and/or services being contracted by the Government Agency, without the enhanced security services.



[REDACTED]

To ensure a seamless installation and testing of services, and the operation and maintenance of those services in accordance with Federal and Agency mandates, the Qwest Team will integrate FEA and National Institute of Standards and Technology (NIST) practices to be fully compliant with FISMA, OMB A-130, and other Federal mandates, while satisfying all RFP requirements.

The Qwest Team is uniquely positioned to provide Agencies with secure, reliable performance that meets MTSS requirements. Focusing on high-end technical aspects of information security solutions in its security business practice areas, we are actively involved in state-of-the-art security technology engineering, design, development, analysis, and consulting efforts for commercial customers and a broad range of defense and civil Government Agencies. Security services range from vulnerability

assessments, penetration tests, technology evaluations, and crisis management to cyber policy, e-commerce, process reengineering, and public key infrastructure.

The Qwest Team has significant experience in evaluating products for Government and commercial use in specified architectures, as well as evaluating products to determine if the products meet specified security and performance criteria. The evaluation experience includes operating the most successful Common Criteria Testing Lab in the United States, using the scheme of the internationally recognized International Organization for Standardization (ISO) 15408 security standard.

**6.8.1.1 Approach to Managed Tiered Security Services Service Delivery (L.34.1.6.1(a))**

The Qwest Team will address security controls and system hardening during design, installation, and operations of Agency MTSS using baseline security guidelines and templates tailored for specific Agency requirements. The Qwest Team will use NIST implementation guidance to help Agencies meet their FISMA requirements and augment these as needed to meet additional compliance requirements using guidance from NSA and the National Information Assurance Program (NIAP).

**Figure 6.8.1-2** shows the FISMA compliance requirements and supporting NIST guidance that the Qwest Team will use in engineering MTSS for specific Agency requirements.

**Figure 6.8.1-2 FISMA Compliance and NIST Guidance**

FISMA Compliance Area	Implementation Reference	Comments
Risk Management	NIST SP 800-30 Risk Management Guide for Information Technology Systems	Manages risks that result from the operation of an information system: enterprise / organizational
Categorization Standard	FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems. NIST SP 800-59 Guideline for Identifying an Information System as a National Security System.	Categorizes information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels
Security Categorization Mapping	NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories	Recommended types of information and information systems to be included in each category
Minimum Security Requirements	FIPS 200 Minimum Security Requirements for Federal Information and Information Systems	Minimum information security requirements for management, operational, and technical security controls for information and information systems in each such category
Minimum Security Controls	NIST SP 800-53, Recommended Security Controls for Federal Information Systems	Minimum security controls (baseline controls for low-impact, moderate-impact, and high-impact information systems) provide a starting point for organizations to select and tailor security controls for specific operational environments used in accordance with organization risk management process.
Security Planning	<ul style="list-style-type: none"> <li>• NIST SP 800-18</li> <li>• Revision 1 Draft Special Publication 800-18</li> <li>• Revision 1, Guide for Developing Security Plans for Federal Information Systems</li> <li>• NIST SP 800-34 Contingency Planning Guide for Information Technology Systems</li> </ul>	Develop, document, and implement an Agency-wide information security program that includes subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate, and includes the security control baselines and requirements traceability.
Security Controls Assessment	<ul style="list-style-type: none"> <li>• NIST SP 800-53A Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems</li> <li>• NIST SP 800-42 Guideline on Network Security Testing</li> </ul>	Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical security controls).
Certification and Accreditation	<ul style="list-style-type: none"> <li>• NIST SP 800-37 Guide for Security Certification and Accreditation of Federal Information Management Systems</li> <li>• NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems</li> </ul>	Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including management, operational, and technical security controls).
Security Program Assessment	<ul style="list-style-type: none"> <li>• NIST SP 800-26 Rev. 1 NIST DRAFT</li> <li>• Special Publication 800-26, Revision 1: Guide for Information Security Program Assessments and System Reporting Form</li> </ul>	Perform an independent evaluation of the information security program and practices to determine the effectiveness of such program and practices.

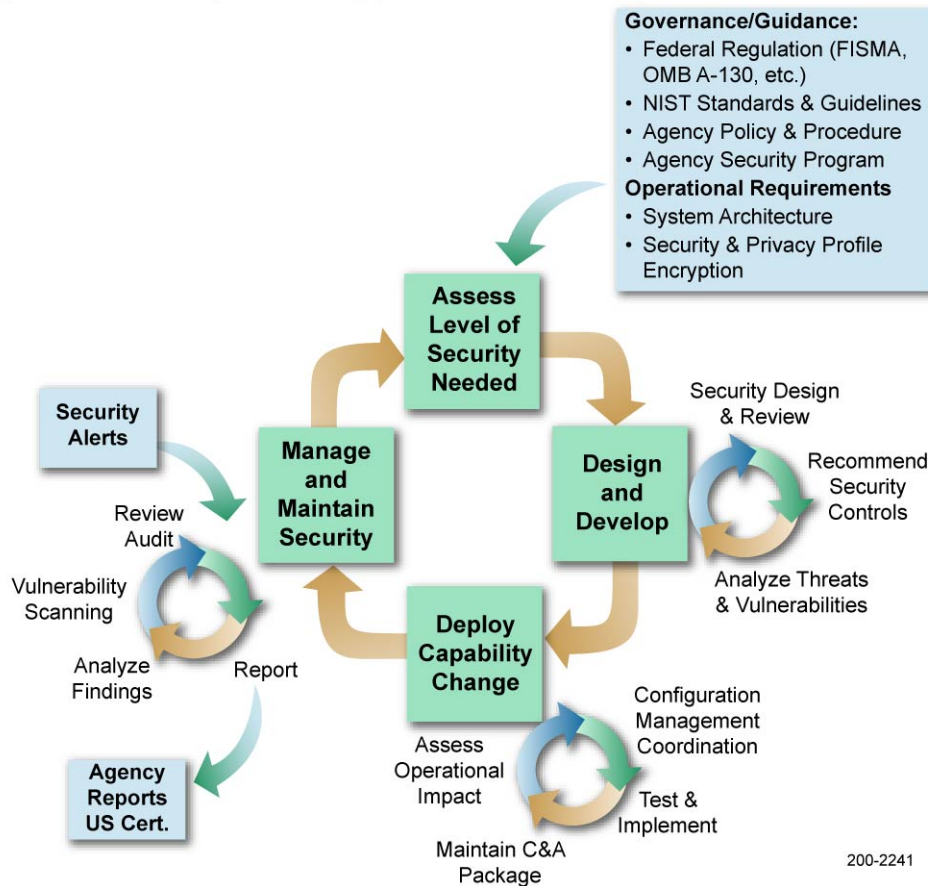
Applying the guidance in the NIST documents to comply with FISMA will result in a more consistent, comparable, and repeatable implementation



of security controls. Any additional requirements consistent with Agency/local policy and “best practices” will be factored into the MTSS delivery.

Consistent and comparable security processes and procedures promote a better understanding of enterprise-wide risks. As more systems connect, authorizing officials need this type of information to make more informed certification decisions. Using the approach described in NIST SP 800-64 Security Considerations in the Information System Development Life Cycle and shown in **Figure 6.8.1-3**, the Qwest Team will use risk management principles to implement required technical, management and operational controls for physical, IT and personnel security.

**Figure 6.8.1-3. Systems Approach to Security**



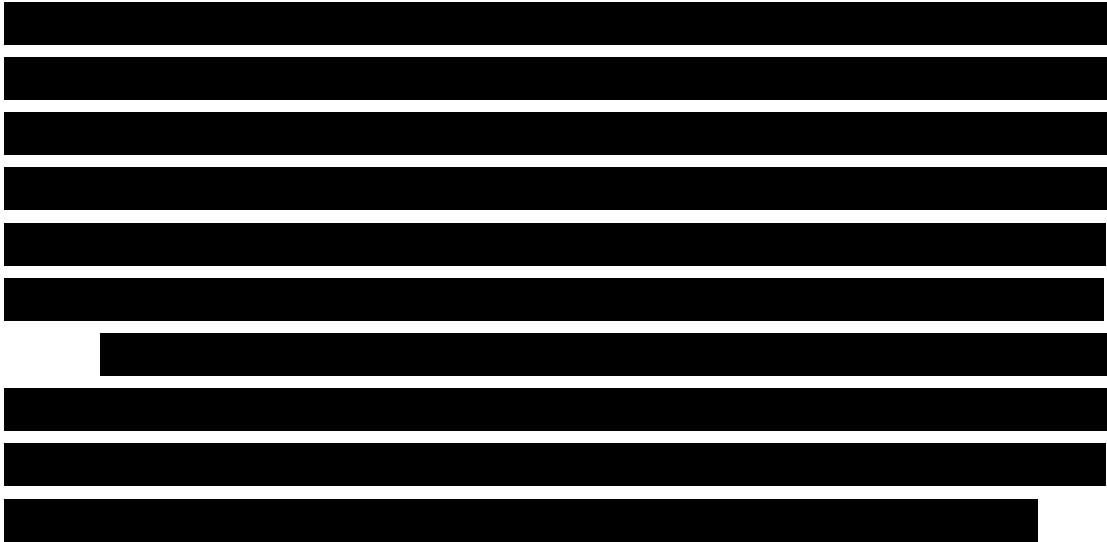


In the Systems Approach to Security, *Assess Level of Security Needed* phase, shown in Figure 6.8.1-3, NIST SP 800-59 Guideline for Identifying an Information System as a National Security System, and NIST FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems, will establish the security requirements for Federal IT systems.

In the Systems Approach to Security, *Design and Development* phase, shown in Figure 6.8.1-3, the FIPS 199 security categorization will form the security requirements baseline in conjunction with the Computer Security Act of 1987, OMB A-130, Appendix III, FISMA, the National Industrial Security Program Operating Manual, NIST SP 800-53, the Agency Enterprise Architect Security and Privacy Profile, and the Agency's security policy to ensure they are satisfied in a coordinated and cost effective manner. The implemented security solution will meet or exceed the baseline established in the system categorization.

The Qwest Team will provide technical, management, and operational controls defined in NIST SP 800-53 (for unclassified systems) as well as Director of Central Intelligence Directives (DCID) 6/3 (for classified systems) to satisfy all system requirements. [REDACTED]

[REDACTED]



In Figure 6.8.1-3, Systems Approach to Security, *Deploy Capability* phase, the Qwest Team will provide on-site installation as required by the requesting Agency. Following the guidelines in NIST SP 800-37 and Agency Certification and Accreditation policies, the Qwest Team will develop Certification and Accreditation packages or provide inputs for systems delivered or operated/maintained for the Agency non-national security systems. The System Security Plan (SSP) and all supporting plans and procedures will be prepared according to NIST SP 800-18 and other applicable guidance, such as NIST SP 800-40 Procedures for Handling Security Patches and NIST SP 800-42 Guidelines for Network Security Testing. The SSP and all system interconnection agreements will be maintained as part of the certification and accreditation package. For national security systems, the Qwest Team will use the DITSCAP or DCID 6/3 guidelines, as appropriate.

The Qwest Security Team will maintain system accreditation in accordance with NIST SP 800-37 and support re-accreditation every three years unless a system change requires earlier re-accreditation. System Interconnection Agreements will be required for all communications and other

interactions that cross the R&D HPCS system boundary developed in accordance with NIST SP 800-47.

The Qwest Team will provide 24x7x365 on-site management and monitoring of service delivery. The requesting Agency will have a shared Web view for authorized Agency personnel to view the topology, operational status, and other management parameters associated with each contracted service.

As part of the Systems Approach to Security, *Manage and Maintain* phase, shown in Figure 6.8.1-3 for service Tiers 2-4, the Qwest Security Team will conduct vulnerability scans of networks in accordance with NIST SP 800-42 Guidelines on Network Security Testing, review security alerts, and analyze the results of scans, audit, and Intrusion Detection Services (IDS). Security patches will be tested following existing procedures for systems upgrades. As new guidance and policies are issued, changes in operational needs occur, or new user requirements are added, the Security Specialists of the Qwest Team will analyze the requirements, adjust security controls as necessary, and implement adjustments to the system security plan to ensure the availability of Agency resources. At a minimum, the NIST SP 800-26 Self Assessment will be completed annually, and risk assessments will be conducted every three years in conjunction with the re-Certification and Accreditation of the system.

When a system or component has reached the end of its useful life or is being replaced as part of the road map and strategy, the disposal process will ensure sensitive information is protected in accordance with NIST SP 800-64.

NIST guidance, as required by FISMA, and any additional requirements levied by Agency/organization policy will be a major input to all security implementations to ensure continued compliance with applicable

governance requirements and the authority to operate issued by the designated approving authority.

The security lifecycle includes several types of security evaluations, including network and vulnerability scanning, risk assessments, and the NIST SP 800-26 Self Assessment. At a minimum, the NIST SP 800-26 Self Assessment will be completed annually, and risk assessments will be conducted every three years in conjunction with the system certification and accreditation, or more frequently as required due to major system changes or increased or materially different threats. The Qwest Team will provide the Agency with a means to manage the risk as required by FISMA. The delivery process begins with a criticality assessment of the business practices and supporting infrastructures, an assessment of the threat, a vulnerability assessment, and, a thorough business continuity and disaster recovery planning. These assessments lead to decisions on mitigation activities to reduce risk. When a system or component has reached the end of its useful life or is being replaced as part of the road map and strategy, the disposal process will ensure sensitive information is protected in accordance with NIST SP 800-64.

Working with system and data owners, as well as users during the MTSS transition phase, Qwest will use the Agency's concept of operations for their IT infrastructure during the preliminary design process to verify the operational requirements and intended use of the system. Some of the basic issues that will be verified include the mission supported by the system, function of the system, data sensitivity, system users and roles, clearances and authorizations required, and initial/anticipated connections.

Using best practices described in NIST SP 800-36 Guide to Selecting Information Security Products, the Team's technical solutions sets apply

products that have been independently evaluated to provide a higher level of assurance. Qwest has used these products successfully for other customers.

Qwest will use cryptographic products that have been evaluated under the FIPS 140-2 and ISA Standard 15408 Common Criteria or other Government recognized independent product evaluation criteria. Common criteria increases assurance and satisfies requirements levied on Federal and DoD organizations by governance documents such as FISMA, NIACAP, DITSCAP, DOD 8500.1 and DOD 8500.2, and HIPAA. [REDACTED]

[REDACTED]

Qwest will use a product's common criteria evaluation and associated security target to help determine if the product has security features and functions necessary to implement an Agency's security requirements and

[REDACTED]

provide expected robustness for Tier 1 – Tier 4 services. The common criteria define seven Evaluation Assurance Levels (EALs), which define the evaluation activities needed to assess a product or system's security. These levels help establish a generalized "level of security" that the component under evaluation provides. EALs balance the level of assurance with the cost and feasibility of acquiring that degree of assurance. The higher the EAL, the higher the degree of assurance that the selected product will satisfy Agency confidentiality, integrity, and availability requirements.

Security accreditation services will be conducted in accordance with NIST SP 800-37, DITSCAP, or DCID 6/3 as required by the Agency, system classification as a national security system, and confidentiality and sensitivity levels. The Security accreditation service provides designated approval authority with the information necessary to make informed decisions on whether the Agency can accept the residual risks and address the requirements of OMB Circular A-130.

Qwest will provide information required by the Agency to integrate MTSS security planning into the Agency information resources management planning process and document procedures in the SSP in accordance with OMB Circular A-130, Appendix III and NIST SP 800-18. The SSP will serve as the primary reference guide for what user security responsibilities are and how users need to satisfy these requirements. The SSP provides necessary guidance, information, and references for rules of behavior, risk assessments, contingency plans, incident response plans, security awareness and training plans, privacy impact assessments, and system interconnection agreements produced as part of an Agency's information security program. The SSP will reference or attach other security-related documents or will prepare or revise necessary security documents to provide guidance on security related to the Agency service level. All plans and procedures will be prepared consistent

with requirements and recommendations in applicable NIST Special Publications.

Qwest will ensure that all changes are analyzed to ensure compliance with the accredited system configuration. Qwest will maintain system accreditation in accordance with NIST SP 800-37, DITSCAP, or DCID 6/3 as required by the Agency. Qwest will support re-accreditation every three years as required by NIST SP 800-37 and DITSCAP, unless a system change requires earlier re-accreditation. System interconnection agreements will be developed in accordance with NIST SP 800-47 for all communications and other interactions that cross the Agency system boundary.

To capitalize on available standardized security testing and certification, Qwest will use a product's common criteria evaluation and associated security target as part of the selection and implementation process. An EAL 4 or below should be sufficient to meet the requirements levied against the system for confidentiality, integrity, and availability for Tier 2. Examining the development processes and using vulnerability testing beginning at EAL 2 provides a level of assurance that a product/system will reliably deliver its specified services with the required level of confidentiality, integrity, and availability. In Tier 3 and Tier 4 environments requiring increased levels of security because of the sensitivity or classification of the data, higher EALs may be required. For example, an EAL 4 database running on an EAL 4 operating system in a protected enclave can be sufficient given the stated threat and environment. However, if an enclave is connected to another enclave that operates at a lower classification, the gateway/guard may require an EAL 5 or above. Depending on the associated risks to confidentiality, integrity, and availability, an EAL 7 product may be more appropriate for Tier 3 and Tier 4 environments, where extremely high risk situations and/or where the high value of the assets justifies the higher costs.



This approach aids Qwest in identifying risks associated with interconnected systems and supporting the certification and accreditation of Tier 1 – Tier 4 MTSS to different Agencies. This management approach to security eases Agency compliance with FISMA security requirements and OMB security and acquisition requirements. This approach minimizes any need for custom-designed components and can be integrated into the Agency asset management and decision process for selection, control, and evaluation. Agencies can use this information to support OMB Exhibit 300s and justify budgets, which is a critical item in the President's Management Agenda eGov scoring process.

**6.8.1.2 Benefits of Managed Tiered Security Services Technical Approach (L.34.1.6.1(b))**

Individual features and benefits of the component services of MTSS can be found in the individual sections of this proposal detailing those services (Sections 6.1 – 6.7).

As a result of the FEA PMO's analysis of the FY 2006 budget data, OMB established the IT Security Line of Business to propose common solutions and architecture, strengthening the ability of all Agencies to identify vulnerabilities, defend against threats, and manage resulting risks. Qwest's MTSS processes and procedures for delivering security service help facilitate FEA objectives such as use of the FEA security and privacy profile methodology to establish an initial set of security controls for a given business process, as shown in **Figure 6.8.1-5**.

**Figure 6.8.1-5. Benefits to Federal Enterprise Architecture Objectives**

Requirement	MTSS Feature and Substantiation
Enhance Cost Savings and Cost Avoidance through a mature FEA Government-wide	Qwest MTSS enhances cost savings and cost avoidance through the adoption of our customized security services practice. Qwest MTSS is a comprehensive portfolio providing the Agency with a robust data protection service that can not be provided by the Agency itself.
Increase cross-Agency and inter-Government collaboration	Qwest MTSS enables Agencies to practice safe inter-Agency communications with the knowledge that Agency networks will be protected and hardened to prevent malicious network intrusions, threats, and attacks.
Improve Utilization of Government Information Resources to focus on core Agency mission and service delivery to citizens by using the FEA	Qwest MTSS provides the Agency with strong data protection services freeing limited Government resources to pursue Agency missions. Our MTSS suite of services will protect Agency networks and limit waste on network threats and disruptions.

**6.8.1.3 Solutions to Managed Tiered Security Service Problems (L.34.1.6.1(c))**

The Qwest Team has detailed knowledge of security principles, threats, technologies, and policies supported by ISO 9000-certified management practices as a result of providing services over the years to our large Federal and commercial customers. This knowledge has been very effective in preventing problems and issues that can cause business interruptions. From our experience, the Qwest Team has learned to effectively anticipate and solve problems that may arise over the service life. These problems have been identified in the individual service sections (see Sections 6.1 to 6.7), and Qwest has proposed our solutions for resolving specific problems associated with individual services in the respective individual service sections.












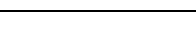

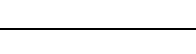
**6.8.2 Satisfaction of Managed Tiered Security Services Performance Requirements (L.34.1.6.2)**

**6.8.2.1 Managed Tiered Security Services Quality of Service (L.34.1.6.2(a))**

[Redacted]

[Redacted]

**Figure 6.8.2-1. Performance Metrics for Qwest MTSS**

Key Performance Indicator		Service Level	Performance Standard (Threshold)	Acceptable Quality Level	
Grade of Service (Configuration/Rule Change)	Routine	Within 5 hours for a normal priority change	≤ 5 hours		
		Within 2 hours for an urgent priority change	≤ 2 hours		
Event Notification	Routine	Within 2 hours of a low category event	≤ 2 hours		
		Within 5 minutes of a high category event	≤ 5 minutes		
Firewall Availability	Routine	99.5 percent of the time	≥ 99.5 percent		
HELP DESK	EN (Outage Notification to Customer)	Routine	Within 2 hours of a low category event	≤ 2 hours	
		Routine	Within 5 minutes of a high category event	≤ 5 minutes	
	GoS (Percentage of Calls Abandoned)	Routine	3 percent	≤ 3 percent	
	Response Time	Routine	All incoming calls to the help desk shall be answered on or before the fifth ring	≤ 5 rings	
AV Multi-level NSA-Approved Security Solution	Routine	100 percent of the time	100 percent		
AV Type 1 Encryption Availability	Routine	99.99 percent of the time	99.99 percent		
Web Portal Availability	Routine	99.7 percent of the time	≥ 99.7 percent		
Event Notification (EN) (Security Incident Reporting)	Routine	Near real-time	≤ 1 hour		

**Grade of Service (GoS)(Configuration/ Change):** Configuration Changes can be requested by the Agency via the Qwest Control Network Portal. Changes initiated by Qwest require Agency consent prior to implementation. Changes are categorized as Normal and Urgent

(emergency). [REDACTED]  
[REDACTED]

**Event Notification (EN):** Qwest's proactive network monitoring capabilities correlates network performance statistics and triggers performance thresholds which automatically create notification trouble tickets in NTM Remedy. [REDACTED]  
[REDACTED]  
[REDACTED]

**Firewall Availability:** Qwest MFS is delivered through industry-leading security appliances which are engineered for [REDACTED]  
[REDACTED]  
[REDACTED]

[REDACTED] Not only are we able to manage real-time appliance environmentals, but actually predict network degradation by monitoring the appliance. Our alert monitoring tools can isolate potential service disruptions prior to full network fault.

**Help Desk Event Notification:** The Agency can notify the help desk via phone, fax, or the NTM Remedy Trouble Ticketing System. To ensure that critical issues are immediately addressed, service levels are set depending on the nature of the event. Below is a description of ticket priorities and their accompanying service level and response times. [REDACTED]  
[REDACTED]  
[REDACTED]

**Help Desk GoS:** [REDACTED]  
[REDACTED] The SOC is staffed 24x7x365 with appropriate number of resources in order to meet the Agency requirements.

**Help Desk Response Time:** [REDACTED]  
[REDACTED] The

SOC is staffed 24x7x365 with appropriate number of resources in order to meet the Agency requirements.

**AV Multi-level NSA-Approved Security Solution:** [REDACTED]

[REDACTED]  
[REDACTED] The Qwest team will use products that have been evaluated under the FIPS 140-2 for cryptographic modules and ISA Standard 15408 Common Criteria or other recognized independent product evaluation criteria. The Qwest team will implement Agency policy and configure the technical solutions using the Common Criteria Protection Profiles and NIST SP 800-70: Security Configuration Checklists Program for IT Products as implementation guidance. Once the controls are designed and developed they are tested and vetted in cooperation with the configuration management team. After security controls are implemented, system security testing is performed to ensure proper and complete implementation.

**AV Type 1 Encryption Availability:** [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] Not only are we able to manage real-time appliance environmental, but actually predict network degradation by monitoring the appliance. Our alert monitoring tools can isolate potential service disruptions prior to full network fault.

[REDACTED]  
[REDACTED]

**Web Portal Availability:** [REDACTED]

[REDACTED]  
[REDACTED]

EN (Security Incident Reporting): Qwest MTSS provides near-real time notification to Agency for incident security reporting. To ensure that critical issues are immediately addressed, service levels are set depending on the nature of the event. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**6.8.2.2 Approach for Monitoring and Measuring Managed Tiered Security Services (L.34.1.6.2(b))**

Qwest's approach is to continually monitor the availability and performance of the key components of the MTSS portfolio. Vital elements of MTSS are monitored for availability and performance by using our multi-dimensional performance monitoring system. This sophisticated, heuristics-

based 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 that are established by the Agency.

The monitoring system alerts the Qwest Team when abnormal security thresholds (threats, violations, virus invasion, brute force attacks, etc.) are violated. Our network health system analyzes communication patterns (baseline usage profiles) of the security appliances to ensure that they are working properly. The network health system is continuously polling the system for jobs and periodically updating and uploading performance data into the SOC via the Security Information Manager (SIM) SOC agent. A deviation from normal communication patterns is escalated to a Qwest SOC engineer for further triage and troubleshooting. All systems in the MTSS platform are monitored via ICMP, SSH, and HTTP probes. A failure to respond to the probe triggers a notification to the Qwest SOC and corrective action is taken.

Agency will have access to all summarized MTSS monitored elements through the Qwest Control Networx Portal. Agency can initiate, view, comment, and close trouble tickets for all MTSS vital elements through this secure, Web-based system.

To ensure AQLs are met and that critical issues are immediately addressed, thresholds are set depending on the nature of the event, in accordance with Federal Information Processing Standards 199 and the NIST 800 series. 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.

Qwest recognizes that it is the Government's intent that KPI monitoring of services is included in the scope of work to be performed. Depending on network topology and policies, additional systems may be required for different security zones to ensure that all critical systems are closely monitored. The SOC lead engineer assigned to the Agency is responsible for monitoring and oversight of the performance of the SLAs. Qwest's delivery experience, combined with our knowledge that each Agency will have unique requirements, especially around Grade of Service, allows the definition of appropriate change control processes and commitment levels by task order AQLs.

[REDACTED]

[Redacted content]

[Redacted text block containing multiple lines of blacked-out content]

[Redacted text block]

[Redacted content]

[Redacted text block]

[Redacted text block]

[Redacted text block]

**6.8.2.4 Managed Tiered Security Services Performance Improvements (L.34.1.6.2(d))**

[Redacted text block]

**6.8.2.5 Additional Managed Tiered Security Services Performance Metrics (L.34.1.6.2(e))**

[Redacted text block]

### **6.8.3 Satisfaction of Managed Tiered Security Services Specifications (L.34.1.6.3)**

Qwest will verify with the Agency requesting services to determine the types of vulnerabilities and threats and the level of security required. In addition, we will provide recommended implementation of security controls for the services specified in Sections 6.1 to 6.7.

#### ***6.8.3.1 Satisfaction of Managed Tiered Security Services Requirements (L.34.1.6.3(a))***

The Qwest Team will select technical solutions that best fit the Agency architecture and security and privacy profile requirements.

##### **6.8.3.1.1 Satisfaction of MTSS Capability Requirements (L.34.1.6.3(a); C.2.7.4.1.5)**

Qwest fully complies with all mandatory stipulated and narrative capabilities, features, and interface requirements for MTSS. [REDACTED] summarizes Qwest's response to the MTSS capabilities listed in RFP C.2.7.4.1.5. This table is intended to summarize the technical capabilities required per L.34.1.6.3(a) and do not limit or caveat Qwest's compliance in any way.

[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]



**6.8.3.1.2 Satisfaction of MTSS Feature Requirements (L.34.1.6.3(a); C.2.7.4.2)**

Qwest fully complies with all mandatory stipulated and narrative capabilities, features, and interface requirements for MTSS. **Figure 6.8.3-2** summarizes Qwest’s response to the MTSS features listed in RFP C.2.7.4.2. This table is intended to summarize the technical features required per L.34.1.6.3(a) and do not limit or caveat Qwest’s compliance in any way.

**Figure 6.8.3-2. Qwest MTSS Features**

ID #	Name of Feature	Description	Approach
1	On-site management and monitoring 24x7x365	The contractor shall provide proactive, around-the clock management and monitoring of the service delivery functions. The Agency shall be able to view the topology, operational state, order status, and other parameters associated with each contracted service.	Qwest will provide On-site management and monitoring 24x7x365. Our NMS and NOC is fully capable and equipped to provide all aspects of alarm monitoring, intrusion detection, and prevention.
2	On-site installation	The contractor shall provide on-site installation services as required by the Agency.	As needed, the on-site installation will either be dispatched or the on-site engineer/technician will perform all installs

**6.8.3.1.3 Satisfaction of MTSS Interface Requirements (L.34.1.4.2(a); C.2.7.4.3)**

Qwest provides all required interfaces based upon the capabilities of our proposed services as defined in: Frame Relay Service (RFP Section C.2.3.1), Asynchronous Transfer Mode Service (RFP Section C.2.3.2),

Internet Protocol Service (RFP Section C.2.4.1), PBIP-VPNS (RFP Section C.2.7.2) and Network-based Internet Protocol VPN (NBIP-VPNS) (RFP Section C.2.7.3).

**6.8.3.2 Proposed Enhancements for Managed Tiered Security Services (L.34.1.6.3(b))**

[REDACTED]

[REDACTED]

**6.8.3.3 Network Modifications Required for Managed Tiered Security Services (L.34.1.6.3(c))**

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

**6.8.3.4 Experience with Managed Tiered Security Services Delivery (L.34.1.6.3(d))**

With [REDACTED] years of designing, developing, implementing and integrating physical and information security and protection for Government and private industry, the Qwest Team has built a unique and operationally robust knowledge base. Our myriad customer activities—including our common criteria laboratory, computer incident response centers, information sharing and analysis centers, and managed security and network operations centers—have given us an international understanding of the challenges facing Governments and industries in a networked world. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[Redacted content]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted content]

[Redacted text block containing multiple paragraphs of blacked-out content]



[REDACTED]

**6.8.3.5 Managed Tiered Security Services Approach (L.34.1.6.3(e))**

MTSS provides an overarching security solution for Agencies depending upon their individual risk models using the tiered approach as described in Section 6.8.1 and called for by GSA requirements. Individual security service designs and their integration into the overall MTSS architecture are shown in the individual service descriptions and technical approaches found in Sections 6.1-6.7.

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 shall also mitigate the potential for Denial of Service (DoS) attacks. Security enhancements include a combination of firewall, premises-based virtual private network (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 SBU mission functions and information. It employs both technical and network management components appropriate to the respective mission and/or information sensitivity.

[Redacted content]