

Figure 4.1.18-1 summarizes the benefits of our solution.

Figure 4.1.18-1. Qwest’s MTIPS Features and Benefits

Feature	Benefit	[REDACTED]
World-class Internet service	High-speed connectivity to the Internet with the same performance as Qwest’s Networkx Internet Protocol Service (IPS)	[REDACTED]
Secure facilities for MTIPS components	Ready-now ability to execute MTIPS requirements	[REDACTED]
World-Class Event Generator architecture that works at Layer 2	Each MTIPS subscriber will get their own complete set of MTIPS security services with no impact or interference by other MTIPS users	[REDACTED]

Feature	Benefit	[REDACTED]
Scalable capacity	Rapid expansion in terms of the number of users as well as data throughput	[REDACTED]
Leverages existing Event Correlation and reporting architecture	Qwest is already using the tools proposed to implement all the SOC functions	[REDACTED]
Flexible access architecture	Agencies have the required flexibility in how they access the TIC Portals	[REDACTED]
Load sharing and dynamic re-route capabilities between TIC Portals as well a critical access	Every MTIPS user gets automatic failover between the two Qwest provided TIC Portals providing extremely robust secure Internet access	[REDACTED]
In-place SOC staff	Qwest has the staff to start providing MTIPS services	[REDACTED]

Qwest has extensive experience in the delivery of IPS services. We apply this experience to ensure the delivery of high-quality IPS to Agencies.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Figure 4.1.18-2 Qwest’s Approach to Common MTIPS Delivery Challenges

Problem	[REDACTED]
Security appliance policy updates, by default, will deny traffic that is not explicitly permitted, which can impact the use of new protocols or	[REDACTED]

Problem	
applications	
Hardware failures or other facility failures	[REDACTED]
"Zero-day" viral activity leaves organizations vulnerable	[REDACTED]
Internet access problems can be hard to identify as they can be from the Internet itself, the managed security equipment in the TIC Portal, access back to the Agency, or due to Agency network problems	[REDACTED]
Firewall Issues	[REDACTED]
Anti-Virus Issues	[REDACTED]
Intrusion Detection and Prevention Issues	[REDACTED]
E-mail Scanning Issues	[REDACTED]

[REDACTED]

4.1.18.2 Satisfaction of MTIPS Performance Requirements (C.2.4.1.5.4)

Figure 4.1.18-3. Qwest Compliance with Performance Metrics for TIC Portal

Key Performance Indicator (KPI)	User Type	Performance Standard (Level/Threshold)	Acceptable Quality Level (AQL)	[REDACTED]
Av(TIC Portal)	Routine Critical	99.5%	≥ 99.5%	[REDACTED]
Grade of Service (Failover Time)	Routine	1 minute	≤ 1 minute	[REDACTED]
Grade of Service (Monitoring and Correlation)	Routine	Real Time	≤ 4 hours 90% of the time	[REDACTED]
	Critical	Real Time	≤ 4 hours 99.9% of the time	
Grade of Service (Configuration/ Rule Change)	Routine	Within 5 hours for a Normal priority change	≤ 5 hours	[REDACTED]
		Within 2 hours for a Urgent priority change	≤ 2 hours	[REDACTED]
EN (Firewall Security Event Notification)	Routine	Within 24 hours of a Low category event	≤ 24 hours	[REDACTED]
		Within 4 hours of a Medium category event	≤ 4 hours	[REDACTED]
		Within 30 minutes of a High category event	≤ 30 minutes	[REDACTED]
EN (Intrusion Detection/ Prevention Security Event Notification)	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 (Virus Updates and Bug Fixes)	Routine	Normal Priority Update 24 hours	≤ 24 hours	[REDACTED]
		Urgent Priority Update 2 hours	≤ 2 hours	[REDACTED]

Figure 4.1.18-4. Qwest Compliance with Performance Metrics for MTIPS Transport Collection and Distribution

Key Performance Indicator (KPI)	User Type	Performance Standard (Level/Threshold)	Acceptable Quality Level (AQL)	[REDACTED]
Av(Port)	Routine	99.95%	≥ 99.95%	[REDACTED]
	Critical	99.995%	≥ 99.995%	[REDACTED]
Latency (CONUS)	Routine	60 ms	≤ 60 ms	[REDACTED]
	Critical	50 ms	≤ 50 ms	[REDACTED]
GOS (Data Delivery Rate)	Routine	99.95%	≥ 99.95%	[REDACTED]
	Critical	99.995%	≥ 99.995%	[REDACTED]
Time to Restore	Without dispatch	4 hours	≤ 4 hours	[REDACTED]
	With dispatch	8 hours	≤ 8 hours	[REDACTED]
EN(Security Incident Reporting)	Routine	Near real time	≤ 30 mins	[REDACTED]

Qwest will use proven mechanisms for measuring the KPI for each of the performance areas, as shown in **Figure 4.1.18-5**.

Figure 4.1.18-5 KPI Measures.

Area	[REDACTED]
Internet Protocol Service and access to the Agency SDP	[REDACTED]
TIC Portal Performance	[REDACTED]

Qwest will follow the guidelines provided in Networx Contract Sections J.13.1 and J.13.2, SLA Measurement Guidelines, as well as the service-independent SLAs in Section J.13.3, SLA Performance Objectives. We will also meet the requirements for credit arrangement in Section J.13.4.

4.1.18.3 Satisfaction of MTIPS Specifications

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

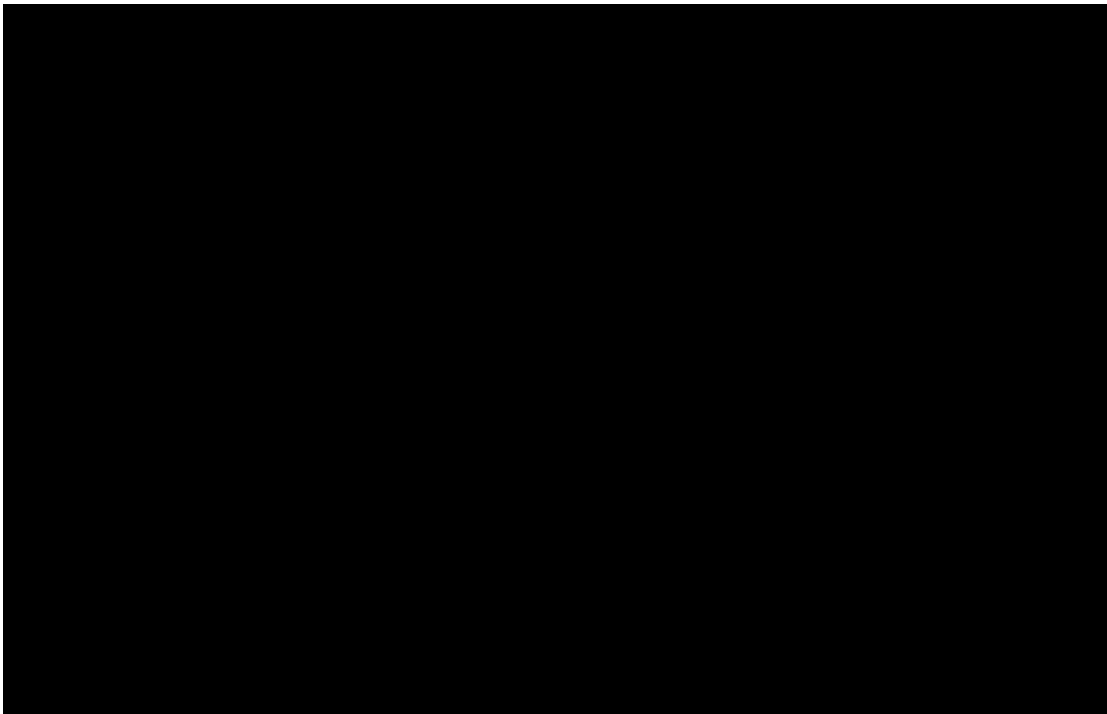


Figure 4.1.18-6. Overall Architecture of the Qwest MTIPS Solution

A more detailed overview of the MTIPS architecture is shown in **Figure 4.1.18-7.**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

[REDACTED]



Figure [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]

Rate of security events	[REDACTED]
Online storage requirements	[REDACTED]
Offline storage requirements	[REDACTED]
Normalized storage requirements Incremental bytes per second required for event storage per Megabit per second of TIC Portal bandwidth	[REDACTED]

To ensure that MTIPS performance metrics and SLAs are met, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4.1.18.3.1 Standards (C.2.4.1.5.1.2)

Qwest's solution has been developed in compliance with the standards identified in the MTIPS Statement of Work (SOW). [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

4.1.18.3.2 Connectivity (C.2.4.1.5.1.3)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4.1.18.3.3 TIC Portal Access to the Internet (C.2.4.1.5.1.4.1-1)

Qwest will provide all of the required access to the Internet.

[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 text block consisting of multiple lines of blacked-out content]

[REDACTED]

[REDACTED]

- **Event Generators (C.2.4.1.5.1.4.1-3p-i)**

[REDACTED]

[REDACTED]

[REDACTED]

Function	
Gateway antivirus	[REDACTED]
IDS and IPS	[REDACTED]
Virtual Private Network Access (Future Feature)	[REDACTED]
Stateful Firewall	[REDACTED]
Anti-Spam	[REDACTED]
Web Content Filtering	[REDACTED]
Bandwidth Shaping	[REDACTED]
Dynamic Threat Prevention	[REDACTED]
Hardened OS	[REDACTED]
Multiple security algorithms and detection techniques	[REDACTED]
Virtual Domain (VDM) technology	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Anomaly Detection for Intrusion Detection & Prevention

(C.2.4.1.5.3-i.4). [REDACTED]

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

[REDACTED]

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

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

[REDACTED]

[REDACTED]

[REDACTED]

- **Anti-Virus Protection Functions (C.2.4.1.5.1.4.1-3p-i.5)**

[REDACTED]

[REDACTED]

[REDACTED]

- **Analysis Engines (C.2.4.1.5.1.4.1-3p-iii).**

[REDACTED]

[REDACTED]

- **System Logs (C.2.4.1.5.1.4.1-3p-iv)**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- **Reporting (C.2.4.1.5.1.4.1-3p-v)**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- Rapid Response Loop Component (C.2.4.1.5.1.4.1-3 (p)(iii) (3) and C.2.4.1.5.1.4.1-3 (q)).

[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]

- **Additional Requirements (C.2.4.1.5.1.4.1-3 (r-u)).**

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

4.1.18.3.6 MTIPS Transport Collection and Distribution (C.2.4.1.5.1.4.2)

[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]

4.1.18.3.7 MTIPS Features Requirements (C.2.4.1.5.2.1)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

ID Number	Name of Feature	[REDACTED]
1	Encrypted Traffic	[REDACTED]
2	Agency Security Policy Enforcement	[REDACTED]
3	Forensic Analysis	[REDACTED]
4	Custom Reports	[REDACTED]
5	Agency NOC/SOC Console	[REDACTED]
6	Customer Certification and Accreditation (C&A) Support	[REDACTED]
7	External Network Connections	[REDACTED]
8	Encrypted DMZ	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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

4.1.18.3.8 MTIPS Interface Requirements (C.2.4.1.5.3.1)

[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]

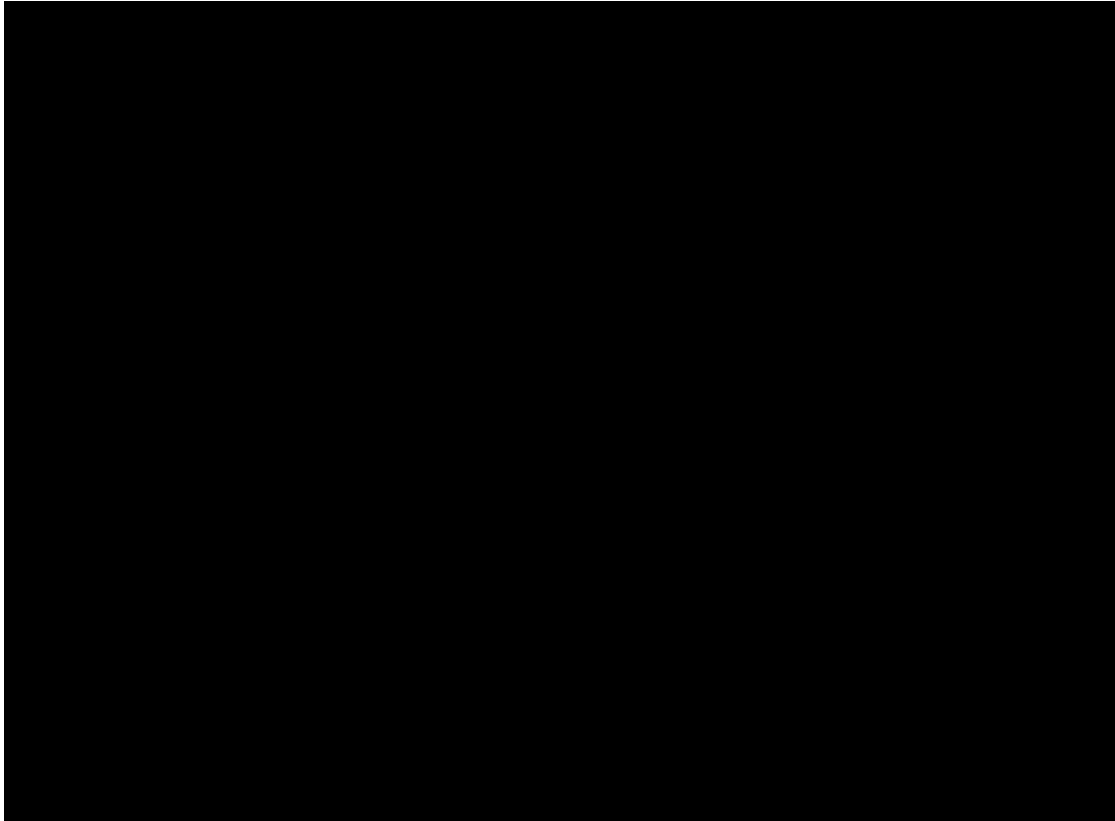
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]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

4.1.18.3.9.2 Security Management (C.2.4.1.5.5.2 and C.2.4.1.5.1.4.1(4))

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4.1.18.3.10 Disaster Recovery (C.2.4.1.5.6)

[REDACTED]

4.1.18.3.11 Service Level Agreements (C.2.4.1.5.7)

[REDACTED]

4.1.18.3.12 TIC Portal SOC FISMA C&A

[REDACTED]

4.1.18.3.12.1 TIC Portal SOC FISMA C&A

[REDACTED]

[REDACTED]

4.1.18.3.12.3 System Security Plan

[REDACTED]

4.1.18.3.12.4 Design Risk/Security Assessment

[REDACTED]

4.1.18.3.12.5 C&A Certification

[REDACTED]

[REDACTED]

4.1.18.3.12.6 Security Test & Evaluation (ST&E)

[REDACTED]

[REDACTED]

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

4.1.18.3.12.7 Security Assessment Process

[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]

The following NIST standards establish the criteria to which the security controls are assessed in the areas of confidentiality, integrity, or availability, and serve as the basis for our security assessments:

- FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- NIST SP 800-30 *Risk Management Guide for Information Technology Systems*, July 2002
- NIST SP 800-53 Revision 2 *Recommended Security Controls for Federal Information Systems*, December 2007
- NIST SP 800-53A *Guide for Assessing the Security Controls in Federal Information Systems*, Second Public Draft, June 2008
- NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004
- NIST SP 800-60 Revision 1 *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008

4.1.18.3.12.8 Accreditation Support

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4.1.18.3.12.9 Configuration Change Management and Continuous Security Monitoring

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4.1.18.3.12.10 Accreditation Documentation

[REDACTED]

4.1.18.3.12.11 C&A Project Management Plan (PMP)

[REDACTED]

4.1.18.3.13 Supply Chain Risk Management (SCRM) Plan (C.2.4.1.5.9)

[REDACTED]

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